Intego NetBarrier X4

Benutzerhandbuch

Intego NetBarrier X4 für den Macintosh

© 1999—2006 Intego. Alle Rechte vorbehalten.

Intego
www.intego.com

Dieses Handbuch enthält die Bedienungsanleitung für die Software Intego NetBarrier X4 für Macintosh. Dieses Handbuch und die Software Intego NetBarrier X4 sind urheberrechtlich geschützt. Alle Rechte vorbehalten. Dieses Handbuch und die Software Intego NetBarrier X4 dürfen nur reproduziert werden, wenn dies in der zugehörigen Softwarelizenzvereinbarung oder schriftlich von Intego genehmigt wurde.

Eigentumsrechte an der Software haben ausschließlich Intego und seine Vorlieferanten. Die Struktur, die Organisation sowie der Quell- und Maschinencode der Software sind Geschäftsgeheimnisse von Intego und seinen Vorlieferanten. Die Software unterliegt US-amerikanischem und internationalem Urheberrecht.

Inhaltsverzeichnis

1 – Über Intego NetBarrier X4 6

Was ist Intego NetBarrier X4? 7

Eigenschaften von Intego NetBarrier X4 7
Persönliche Firewall 7
Antivandalismus 7
Schutz persönlicher Daten 9
Überwachung 10

Über dieses Benutzerhandbuch 11

2 – Einführung in die Datensicherheit 12

Weshalb Ihr Computer unbedingt vor Angriffen geschützt werden sollte 13

Wie kann ein Computer vollkommen sicher gemacht werden? 14
Was ist eine Firewall? 15
Freund oder Feind? 15

Was Sie riskieren 16

Weshalb Leute in Computersysteme eindringen 16
Die unterschiedlichen Arten möglicher Angriffe und Eindringversuche 17

Schutz persönlicher Daten 18

3 – Installation 20

Systemanforderungen 21

Installieren von Intego NetBarrier X4 21

So registrieren Sie Intego NetBarrier X4 26

Verwenden von Intego NetBarrier X4 im Demonstrationsmodus 27

4 – Erste Schritte 29

Verwenden von Intego NetBarrier X4 30

Verwenden des Hauptfensters von Intego NetBarrier X4 30

Verändern der Größe des Fensters von NetBarrier X4 33

Einrichten der Firewall 34

Verwenden des Menüs von NetBarrier X4 39

Intego Widgets 41

Passwortschutz von Intego NetBarrier X4 42

Aufrufen von Hilfeinformationen 42

Links zur Website von Intego 42

5 – Die vier Verteidigungslinien 43

Firewall 44

Firewall-Einstellungen 45
Protokoll 48

Schutz vor Trojanischen Pferden....68

Antivandalismus....70
Richtlinie....71
Einstellen der Empfindlichkeit gegenüber Ping-Überflutung....75
Einstellen der Empfindlichkeit gegenüber Port-Scans....76
Einstellen der Empfindlichkeit gegenüber SYN-Überflutung....77

Warnmeldungen....78
Angriffszähler....81
Warnmeldungen....82
Die Sperrliste....85
Vertrauenswürdige Gruppe....99

Anti-Spyware....113
Verwenden der Registerkarte „Anti-Spyware“....114
Optionen....116

Schutz persönlicher Daten....123
Datenfilter....124
Banner-Filter....135
Cookie-Manager....140
Säubern von Webbrowserdateien....146
Surffilter....148

Überwachung....153
Datenverkehr....153
Verwenden des Programms NetBarrier-Monitor....169
Das Widget für NetBarrier-Monitor....173
Der Bildschirmschoner von Intego NetBarrier X4....174
Dienste....177
Netzwerk....179
Whois....184
Traceroute....185

NetUpdate....188

6 – Voreinstellungen und Konfigurationen....189

Voreinstellungen von Intego NetBarrier X4....190
Modem....190
Einstellungen für Protokollexport....191
Einstellungen für Datenverkehrexport....197
Whois....202
Erweiterte Optionen....204

Über Intego NetBarrier X4....205

Konfigurations-Manager....206
Auswählen der aktiven Konfiguration....207
Hinzufügen von Konfigurationssätzen....207
Löschen von Konfigurationssätzen....209
Umbenennen von Konfigurationssätzen....210
Exportieren von Voreinstellungen....211
Importieren von Voreinstellungen....211

7 – Individuell konfigurierter Schutz *212*

Verwenden des Modus „Benutzerdefiniert“ von Intego NetBarrier X4 ..... **213**

Vom Benutzer konfigurierbare Firewall-Optionen 214

Reihenfolge der Firewall-Regeln 214

Definieren von Regeln mit dem Regelassistenten **216**

Definieren von Regeln **226**

Datenziele 237

Dienste 243

Schnittstellen 250

Dienste-Bibliothek 254

Löschen von Regeln 255

Ändern von Regeln 255

Verwenden der Funktion „Auswerten der Regeln anhalten“ 256

Verwenden des Kontextmenüs für Regeln 257

8 – Technische Unterstützung *260*

9 – Glossar *263*

1 – Über Intego NetBarrier X4

Was ist Intego NetBarrier X4?

Intego NetBarrier X4 ist die perfekte Internet-Sicherheitslösung für Macintosh-Computer mit dem Betriebssystem Mac OS X. Dieses Softwareprodukt bietet umfassenden Schutz vor Versuchen, übers Internet oder ein lokales Netzwerk in Ihren Computer einzudringen.

Intego NetBarrier X4 schützt Ihren Computer vor Eindringversuchen, indem alle vom Internet oder einem anderen Netzwerk eingehenden und alle ausgehenden Datenpakete kontinuierlich gefiltert werden. Mit Intego NetBarrier X4 sind Sie vor Datendiebstahl, Hackerangriffen und Eindringversuchen geschützt. Die Software warnt sie automatisch bei verdächtigen Aktivitäten.

Eigenschaften von Intego NetBarrier X4

Intego NetBarrier X4 stellt vier separate Verteidigungslinien auf, um Ihren Computer vor Eindringversuchen und Angriffen zu schützen.

Persönliche Firewall

Intego NetBarrier X4 enthält eine persönliche Firewall, die alle ein- und ausgehenden Datenpakete filtert. Standardmäßig stehen mehrere grundsätzliche Filterregeln zur Verfügung. Im Modus „Benutzerdefiniert“ können Sie bei Bedarf Ihre eigenen Regeln definieren.

Antivandalismus

Die in Intego NetBarrier X4 integrierte Funktion „Antivandalismus“ ermöglicht es Ihnen, Ihren Computer gegen Angriffe durch Vandalen abzuschotten. Diese Funktion überwacht die Netzwerkaktivitäten Ihres Computers auf Anzeichen von

Eindringversuchen, stoppt diese und gibt eine entsprechende Warnmeldung aus. Die Funktion „Antivandalismus“ protokolliert die Internet-Adressen aller Eindringlinge und sperrt diese, sodass weitere Eindringversuche unmöglich gemacht werden. Intego NetBarrier X4 stellt Ihnen mehrere Optionen zur Verfügung, um die Software an Ihre jeweiligen Anforderungen anzupassen.

Warnmeldungen

Intego NetBarrier X4 sperrt alle eingehenden Datenpakete, die als feindlich betrachtet werden. Intego NetBarrier X4 kann ein Dialogfeld mit einer Warnmeldung öffnen, woraus hervorgeht, weshalb die Datenpakete gesperrt wurden. Gleichzeitig werden Sie aufgefordert, den Empfang der Datenpakete zu erlauben oder zu verweigern. Sie können auch andere Alarmoptionen wählen. Beispielsweise können Sie festlegen, dass ein akustischer Alarm ausgegeben werden soll, dass die Internet-Adresse des sendenden Computers in die Sperrliste aufgenommen werden soll, oder dass an die von Ihnen vorgegebenen E-Mail-Adressen eine E-Mail-Mitteilung mit einer Warnmeldung gesendet werden soll.

Sperrliste

Wenn Intego NetBarrier X4 erkennt, dass jemand versucht, übers Netzwerk in Ihren Computer einzudringen, können Sie die Internet-Adresse des anderen Computers in die Sperrliste aufnehmen lassen. Wenn später ein Computer mit der gleichen Internet-Adresse eine Verbindung mit Ihrem Computer herstellen will, so wird dieser Zugriffsversuch automatisch gesperrt.

Vertrauenswürdige Gruppe

Es kann vorkommen, dass Ihnen bekannte Computer – Freunde, keine Feinde – von Intego NetBarrier X4 gesperrt werden. Hierbei kann es sich um Computer in Ihrem lokalen Netzwerk handeln, die beispielsweise nur deshalb gesperrt werden, weil sie Ihren Computer „anpingen“. Mit Intego NetBarrier X4 können Sie die

Internet-Adressen dieser „befreundeten“ Computer als Computer einer vertrauenswürdigen Gruppe deklarieren. So stellen Sie sicher, dass die Computer in Ihrem Netzwerk auf Ihren Computer zugreifen können. Beachten Sie auf jeden Fall, dass die Vertrauenswürdige Gruppe nur für die Antivandalismus-Funktion von Intego NetBarrier X4 gilt und dass die Firewall-Regeln auf die Computer in der Vertrauenswürdigen Gruppe angewendet werden.

Anti-Spyware

Intego NetBarrier X4 ermöglicht es Ihnen, festzulegen, welche Programme aufs Internet und/oder auf Ihr lokales Netzwerk zugreifen dürfen. Wenn ein nicht vertrauenswürdiges Programm versucht, aufs Netzwerk zuzugreifen kann Intego NetBarrier X4 eine Warnmeldung ausgeben, um Sie darüber zu informieren, welches Anwendungsprogramm versucht, die Verbindung herzustellen. Wenn Sie dem betreffenden Anwendungsprogramm den Zugriff erlauben wollen (wenn es wirklich ein Programm ist, von dem Sie wissen, dass es das Netzwerk verwenden sollte), können Sie dies tun. Wenn ein Programm aber ohne Ihr Wissen eine Netzwerkverbindung herstellen will, können Sie ihm auf Dauer den Netzwerkzugriff verwehren.

Schutz persönlicher Daten

Intego NetBarrier X4 bietet Ihnen auch einen Schutz Ihrer persönlichen Daten. Das Programm filtert die Daten und stellt so sicher, dass keine sensiblen Informationen Ihren Computer verlassen. Es blockiert zudem Werbebanner und Sie können damit Cookies verwalten und diese zu jedem beliebigen Zeitpunkt löschen. NetBarrier X4 kann auch den Cache Ihres Webbrowsers und die Surfprotokolle (Dateien mit Informationen über besuchte Websites) löschen. Ferner kann Intego NetBarrier X4 Informationen über Ihren Computer verbergen: das Betriebssystem, den verwendeten Webbrowser und die zuletzt von Ihnen aufgerufene HTML-Seite.

Überwachung

Intego NetBarrier X4 ermöglicht Ihnen die umfassende Überwachung Ihrer Netzwerkaktivitäten. Die grafischen Messskalen zeigen das Netzwerk-Datenverkehrsaufkommen in Echtzeit an. Ferner werden Informationen über Ihren Computer, das lokale Netzwerk sowie aktive Dienste und Verbindungen angezeigt.

Intego NetBarrier X4 enthält auch einen eigenen Bildschirmschoner, mit dem Sie den Datenverkehr Ihres Computers auch dann im Blick behalten, wenn ein Bildschirmschoner aktiviert ist.

Über dieses Benutzerhandbuch

Sie sind:

- **Eine Privatperson mit Internet-Zugang**

  Wenn Obiges auf Sie zutrifft, sollten Sie zuerst das Kapitel 2, **Einführung in die Datensicherheit**, und dann die Kapitel 3, **Installation**, und 4, **Kurzanleitung**, lesen. Wenn Sie der Meinung sind, ausreichend über dieses Thema informiert zu sein, können Sie an dieser Stelle aufhören, denn Intego NetBarrier X4 schützt Ihren Computer automatisch vor Eindringversuchen. Wenn Sie aber mehr wissen wollen, lesen Sie bitte das Kapitel 5, **Die vier Verteidigungslinien**.

- **Ein Mitarbeiter eines Unternehmens oder einer anderen Organisation mit Anschluss an ein lokales Netzwerk und das Internet**

  Wenn Ihr Computer mit einem lokalen Netzwerk verbunden ist, sollten Sie die weiter oben angegebenen Kapitel dieses Benutzerhandbuchs ebenfalls lesen. Die Basismodi von Intego NetBarrier X4 dürften auch für Sie ausreichen.

- **Ein Benutzer, der seinen Computer als Server betreibt oder ein Netzwerk verwaltet**

  Sie sollten das ganze Benutzerhandbuch durchlesen. Von besonders großer Bedeutung für Sie dürfte das Kapitel 7, **Individuell konfigurierter Schutz**, sein. Hier erfahren Sie, wie Sie eigene Firewall-Regeln definieren können.

Am Ende dieses Handbuchs finden Sie eine Liste häufig verwendeter Fachbegriffe.

2 – Einführung in die Datensicherheit

Weshalb Ihr Computer unbedingt vor Angriffen geschützt werden sollte

Unabhängig davon, ob Sie Ihren Computer zum Arbeiten oder nur zum Surfen im Internet verwenden, ob Sie den ganzen Tag über oder nur ab und zu online sind, ob Ihr Computer isoliert oder mit einem lokalen Netzwerk verbunden ist, ob Sie Privatperson oder Mitarbeiter eines Unternehmens oder einer anderen Organisation sind: Ihr Computer enthält sensible und damit schützenswerte Informationen. Bei diesen Informationen kann es sich um Ihre Kreditkartennummer, Ihre Bankkontodaten, Verträge mit Kunden oder Mitarbeitern, Dokumente zu vertraulichen Projekten oder um E-Mail-Mitteilungen oder Passwörter handeln. Ganz egal, welche vertraulichen Informationen Sie auf Ihrem Computer gespeichert haben: irgendwo da draußen in den Weiten des Internet gibt es bestimmt jemanden, der sich dafür interessieren könnte.

Je intensiver Sie Ihren Computer für Ihre tägliche Arbeit oder Ihr Hobby nutzen, umso mehr Informationen sind darauf gespeichert, die vor dem Zugriff durch Unbefugte geschützt werden sollten.

Vergleichen Sie einfach Ihren Computer mit einem Haus! Bevor Sie Ihr Haus verlassen, werden Sie höchstwahrscheinlich alle Fenster schließen und alle Türen absperren. Aber schützen Sie Ihren Computer auf die gleiche Weise? Solange Ihr Computer mit einem Netzwerk verbunden ist, können raffinierte Hacker und Kriminelle auf die Daten zugreifen, die auf Ihrem Computer gespeichert sind. Es sei denn, Sie verwenden Intego NetBarrier X4 zum Schutz Ihres Computers.

Wenn Ihr Computer mit einem Netzwerk verbunden ist - ganz gleich, ob Sie ihn nur privat nutzen, er in ein Netzwerk integriert ist, oder er mit dem Internet verbunden ist: er ähnelt prinzipiell einen Haus an einer Straße mit Türen und Fenstern. Intego NetBarrier X4 funktioniert wie ein Schloss und schützt auf diese Weise Ihre Türen und Fenster. Wenn Sie eine HTML-Seite aufgerufen haben, wissen Sie niemals, wer dies

beobachten kann. Wenn Sie beispielsweise auf eine Website mit Informationen über Computerspiele gehen und dort nach Tricks suchen, wie Sie Ihre Gegner überlisten können, lauert dort vielleicht ein Hacker aufs Sie, der Ihren Computer ausspionieren ihren will, um zu sehen, ob er etwas von Interesse finden kann. Ein anderer denkbarer Fall wäre, dass Sie eine Website mit Aktienkursinformationen besuchen, die von einem Hacker überwacht wird, der nun versucht, die Computersysteme der Websitebesucher „nur zum Spaß“ zu beschädigen.

Ohne Intego NetBarrier X4 werden Sie vielleicht nie erfahren, ob irgendjemand versucht, auf Ihre Daten zuzugreifen.

Ein Computer ist nur so sicher wie die Leute, die Zugriff darauf haben. Intego NetBarrier X4 schützt Ihren Computer, indem der Zugriff vom Netzwerk durch Unbefugte sowie das Versenden sensibler Informationen gesperrt wird.

Wie kann ein Computer vollkommen sicher gemacht werden?

Es gilt als allgemein bekannt, dass ein Computer nur sicher gemacht werden kann, indem man ihn ausschaltet, alle Verbindungen mit ihm abtrennt, ihn in einem mit Titan verstärkten Safe verschließt, diesen in einem atombombensicheren Bunker einmauert, die äußeren Räume mit Giftgas erfüllt und vor dem Bunker hoch bezahlte, bewaffnete Wachen postiert. Da dies nun einmal sehr unpraktisch ist, muss eine andere Lösung gesucht werden. Schließlich wollen Sie in der Lage sein, mit Ihrem Computer zu arbeiten.

Die optimale Lösung dieses Problems ist Intego NetBarrier X4. Diese Software bietet Ihnen Schutz, der weit über das hinausgeht, was die meisten Computer-Benutzer benötigen. Durch seine auf einfachste Weise an jede Situation anpassbaren Firewall-Regeln ist Intego NetBarrier X4 das perfekte Hilfsmittel für System- und

Netzwerkverwalter, die damit in der Lage sind, dem Schutze an Ihre spezifischen Anforderungen anzupassen.

Was ist eine Firewall?

Eine Firewall (deutsche Übersetzung: Brandschutzmauer) funktioniert wie eine Wand. Sie schützt Ihren Computer oder Ihr lokales Netzwerk, indem Benutzer in zwei Gruppen untergliedert werden: diejenigen innerhalb der Wand und die anderen außerhalb. Eine Firewall wird so konfiguriert, dass Personen außerhalb der Firewall nur unter bestimmten Bedingungen Zugriff auf die Computer innerhalb der Firewall haben können. Das Gleiche gilt auch umgekehrt.

Eine Firewall ist eine Art Filter zwischen Ihrem Computer oder LAN (Local Area Network = lokales Netzwerk) und einem WAN (Wide Area Network = Weitverkehrsnetz) wie dem Internet. Die Firewall filtert Datenpakete und prüft, woher sie kommen und wohin sie gehen.

Mit Intego NetBarrier X4 können fortgeschrittene Benutzer eigene Filterregeln definieren, um ihre Computer vor Eindringversuchen zu schützen.

Freund oder Feind?

Damit jemand durch eine Wand gehen kann, muss diese eine Tür enthalten. Die Funktion „Antivandalismus“ von Intego NetBarrier X4 fungiert als Filter oder Wachpersonal, das die Tür einer Wand bewacht und alle ein- und ausgehenden Daten auf Anzeichen von Hackern, Vandalen, Spionen, Eindringlingen und Dieben prüft. Dies ist möglich, da in ein ungeschütztes Computersystem auf mehrere unterschiedliche Weisen eingedrungen werden kann, und Intego NetBarrier X4 diese Verfahren erkennt.

Was Sie riskieren

Weshalb Leute in Computersysteme eindringen

Dafür, dass manche Leute in fremde Computersysteme einzudringen versuchen, gibt es mehrere Gründe. Manchmal versuchen Hacker, von fremden Computern aus in andere Computersysteme einzudringen, um ihre Spuren zu verwischen. Dies ist möglich, indem Verbindungen zwischen so vielen Computersysteme wie möglich hergestellt werden, sodass der Computer, von dem aus der Hacker operiert, nicht identifiziert werden kann.

Andere Leute versuchen, in fremde Computersysteme einzudringen, weil ihnen dies Spaß macht und sie immer neue Möglichkeiten dazu herausfinden müssen. Dies ist so ähnlich wie mit den Graffitisprayern, die ihre „Kunstwerke“ oftmals nur in die Welt setzen wollen, damit diese wahrgenommen werden.

Allerdings gibt es auch richtige Kriminelle, die versuchen, in Computer anderer Leute einzudringen. Hierbei kann es sich um Wirtschaftsspione handeln, die Informationen über Aktivitäten, Projekte und Kunden eines Konkurrenzunternehmens ausspähen wollen. Oder um Diebe, die Passwörter und Kreditkartennummern ausspionieren, um sich geldwerte Vorteile zu verschaffen. Die meisten Unternehmen haben Richtlinien zur Datensicherheit ausgearbeitet, doch nur wenige Unternehmen kümmern sich um die Sicherheit ihrer Unternehmensdaten auf den Privatcomputern ihrer Mitarbeiter. Viele Angestellte arbeiten auch zuhause für ihr Unternehmen, sodass auch die Privatcomputer von Mitarbeitern geschützt werden müssten.

Unglücklicherweise leben wir in einer Welt, in der sich fast alles zu Geld machen lässt. Da die heutige Wirtschaft vor allem auf Informationen basiert, ist es kein Wunder, dass es heutzutage lukrativer ist, Informationen als Edelmetalle zu stehlen. Hier ist ein einfaches Beispiel: Am Muttertag im vergangenen Jahr haben Sie Ihrer Mutter oder Ihrer Gattin Blumen gekauft. Diese hatten Sie per Fax bestellt, da Sie Ihre

Kreditkartennummer nicht übers Internet versenden wollten. Da Sie das Fax von Ihrem Computer aus versandt haben, ist das gefaxte Dokument mit der Kreditkartennummer immer noch auf der Festplatte Ihres Computers gespeichert. Wenn nun jemand beispielsweise übers Internet in Ihr Computersystem eindringt, kann er dieses Dokument auf seinen Computer kopieren und mit Ihren Kreditkartenangaben Einkäufe zu Ihren Lasten tätigen.

Die unterschiedlichen Arten möglicher Angriffe und Eindringversuche

Es gibt viele Gründe, aus denen Leute versuchen, in die Computersysteme anderer einzudringen. Und es gibt vermutlich ebenso viele Verfahren, um dies zu tun. Einige Gründe sind folgende:

- Das „Stehlen“ vertraulicher Dokumente und Informationen.
- Das Ausführen von Befehlen auf Ihrem Computer, um das Betriebssystem zu verändern, Ihre Festplatte zu löschen oder Ihren Computer auf sonstige Weise zu beschädigen.
- Das Verfremden von Websites durch Ersetzen von HTML-Seiten durch anderen Text und/oder andere Grafiken.
- Das Durchführen von DoS-Angriffen (DoS, Denial of Service = Dienstverweigerung) mit dem Ziel, einen fremden Computer so mit Datenpaketen zu überschwemmen, dass er auf keine anderen Anfragen mehr reagieren kann.
- Das Erfassen von Informationen über Ihren Computer, um einen späteren Versuch eines Eindringens in Ihr Netzwerk oder Ihren Computer zu starten.

Schutz persönlicher Daten

Sie werden vermutlich nicht wissen, wie viele Informationen über Sie von Websites abgefragt werden, wenn Sie ganz normal im Internet surfen. Beim Besuch mancher Websites werden Sie gebeten, sich anzumelden. Hier müssen Sie einen Benutzernamen und ein Passwort eingeben. Gelegentlich werden Sie auch aufgefordert, Ihren Namen, Ihre Postadresse und andere Informationen einzugeben. Diese Informationen werden häufig dazu verwendet, Ihr Surfverhalten und Ihre Interessen zu analysieren, um Ihnen speziell auf Ihre Wünsche zugeschnittene Produkte und Dienstleistungen anzubieten.

Immer mehr Internet-Benutzer weigern sich, den Betreibern von Websites persönliche Informationen zur Verfügung zu stellen. Manchmal gibt es hierfür auch einen wirklich triftigen Grund: Sie melden sich beispielsweise bei einer Website an, und später erhalten Sie unaufgefordert eine Vielzahl von Werbemitteilungen per E-Mail. Wenn dies geschieht, ist es allerdings meistens zu spät.

Website-Server können aber auch noch andere Informationen über Sie und Ihr Verhalten abfragen. Wussten Sie, dass Ihr Webbrowser bei jedem Besuch einer Website Informationen darüber versendet, welches Betriebssystem und welchen Webbrowser Sie verwenden, und sogar, welche HTML-Seite Sie als letzte aufgerufen haben?

Ein weiteres Problem stellen so genannte Cookies dar. Hierbei handelt es sich um eine kleine Datei, die ein Website-Server auf der Festplatte Ihres Computers speichert. Beim nächsten Besuch der gleichen Website wird das Cookie von Ihrem Webbrowser an eben diesen Website-Server zurückgesandt. Typischerweise werden Cookies dazu verwendet, um einen Benutzer wieder zu erkennen, nachdem er sich einmal bei einer Website angemeldet hat. Dadurch müssen die Anmeldeinformationen wie Benutzername und Passwort nicht mehr eingegeben werden. Cookies werden auch dazu verwendet, um den Einkauf im Internet zu vereinfachen. So können Sie zunächst Ware auf einer Website auswählen und in einen virtuellen „Einkaufswagen“ legen. Dank dem Cookie weiß der Website-Server später, welche Produkte oder Dienstleistungen Sie erwerben wollen,

bevor es an die Bezahlung geht. Ein Cookie ermöglicht es auch, zu erkennen, welche Seiten einer Website Sie aufgerufen haben, sodass Ihnen auf Ihre persönlichen Vorlieben abgestimmte Seiten angeboten werden.

Cookies haben durchaus ihre Berechtigung, können aber auch zum Analysieren Ihres Surfverhaltens verwendet werden. Diese Daten werden dann unter Umständen an Unternehmen verkauft, die Ihnen nun Produkte und Dienstleistungen anbieten, die zu Ihrem individuellen Surfverhalten passen. Es kommt sogar vor, dass die Banner, die Sie beim Besuch von Websites zu sehen bekommen, auf Grund dieser gesammelten Informationen über Ihr Surfverhalten aktiviert werden.

Intego NetBarrier X4 bietet Ihnen auf einfachste Weise einen umfassenden Schutz Ihrer persönlichen Daten: Sie können festlegen, dass bestimmte Informationen über Sie nicht von Ihrem Computer gesendet werden können.

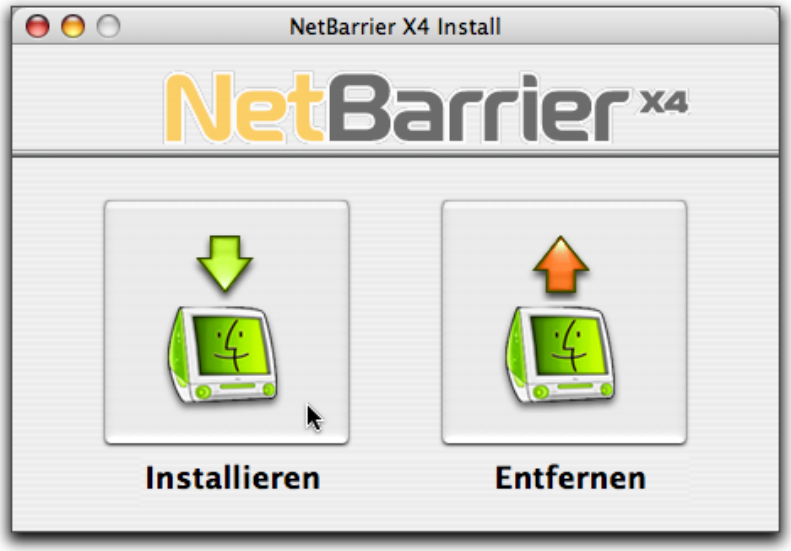
3 – Installation

Systemanforderungen

- Jeder mit Mac OS X kompatible Macintosh
- Mac OS X 10.2.8 oder neuer, Mac OS X Server 10.2.8 oder neuer
- Freie Festplattenspeicherkapazität von mindestens 40 MByte
- Bildschirmdarstellung von minimal 800 x 600 Bildpunkten

Installieren von Intego NetBarrier X4

Wenn Sie das Installationsprogramm von NetBarrier X4 aus dem Internet heruntergeladen haben, suchen Sie die heruntergeladene Datenträgerabbilddatei. Doppelklicken Sie auf den Ordner für die Sprachversion, die Sie installieren möchten. Doppelklicken Sie anschließend auf das Symbol des Programms „NetBarrier X4 Installer“. Es wird Ihnen dann ein Fenster angezeigt, indem Sie die Optionen „Installieren“ oder „Entfernen“ auswählen können: Klicken Sie auf „Installieren“.



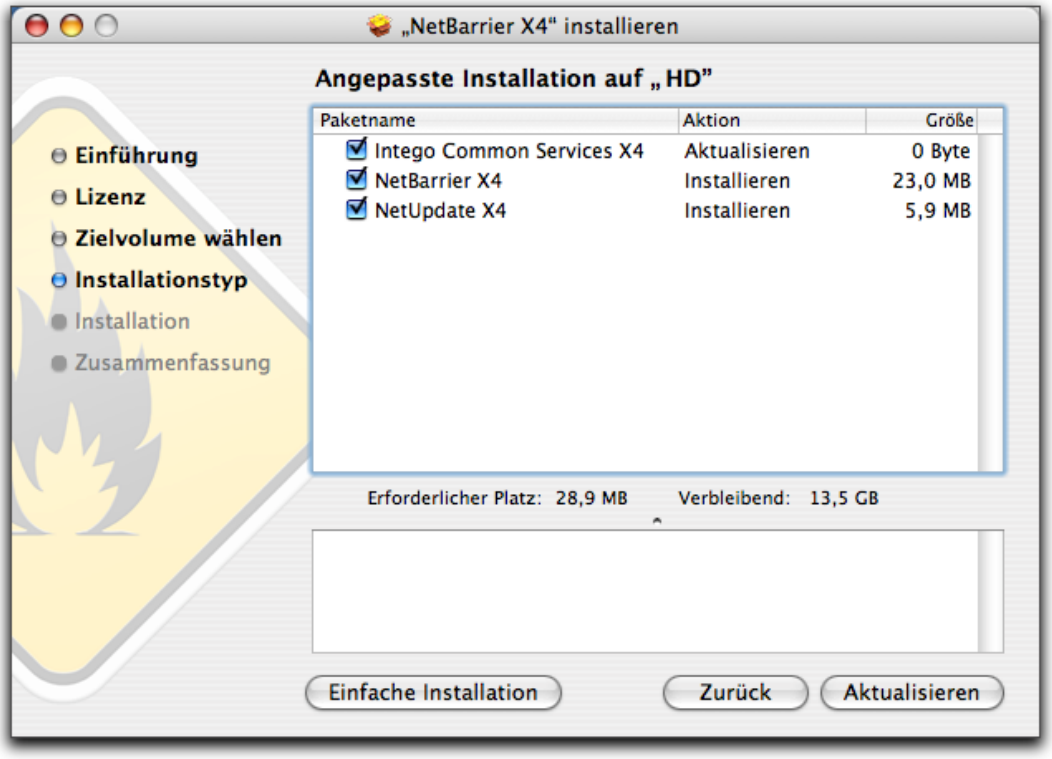
Wenn Sie eine verpackte Version von NetBarrier X4 gekauft haben, legen Sie die Intego-CD in Ihren Computer ein. Anschließend wird ein Fenster geöffnet. Doppelklicken Sie auf den Ordner für die Sprachversion, die Sie installieren möchten. Doppelklicken Sie dann auf das Symbol „Intego Software Install“. Es wird ein Fenster geöffnet, indem Sie darauf hingewiesen werden, dass Sie zur Installation der Software eine Seriennummer benötigen. Sie können auch eine Demoversion ohne Seriennummer installieren. Klicken Sie auf die Schaltfläche „OK“. Wählen Sie aus der Dropdownliste von NetBarrier X4 die Option „Installieren“. Auf dem Symbol von NetBarrier X4 wird Ihnen dann ein grüner Pfeil eingeblendet, der anzeigt, dass Sie die Installation dieser Software ausgewählt haben. Klicken Sie dann auf die Schaltfläche „Installation starten“.

Sie müssen das Kennwort eines Administrators eingeben, um Intego NetBarrier X4 auf Ihrem Computer installieren zu können.

Klicken Sie auf die Schaltfläche „Fortfahren“, um die Installation fortzusetzen. Nun wird die Intego-Softwarelizenzvereinbarung angezeigt. Klicken Sie zuerst auf die Schaltfläche „Fortfahren“ und dann auf die Schaltfläche „Annehmen“, um die Bedingungen der Intego-Softwarelizenzvereinbarung zu akzeptieren. Wenn Sie die Intego-Softwarelizenzvereinbarung nicht akzeptieren wollen, müssen Sie auf die Schaltfläche „Ablehnen“ klicken, worauf das Installationsprogramm automatisch beendet wird.

Im nächsten Fenster sehen Sie die Symbole aller für Ihren Computer verfügbaren Datenträger. Wählen Sie den Datenträger, auf dem Intego NetBarrier X4 installiert werden soll, und klicken Sie dann auf die Schaltfläche „Fortfahren“.

Klicken Sie auf die Schaltfläche „Aktualisieren“, um Intego NetBarrier X4 zu installieren. Hierbei werden die notwendigen Komponenten von NetBarrier X4 installiert. Wenn Sie eine benutzerspezifische Installation durchführen wollen, müssen Sie auf die Schaltfläche „Anpassen“ klicken. Nun wird das folgende Fenster geöffnet:



In diesem Fenster können Sie die zu installierenden Softwarekomponenten wählen. Sie können auswählen, ob Intego Common Services X4, Intego NetBarrier X4, NetUpdate X4 oder all diese Elemente installiert werden sollen.

Nach der Installation müssen Sie Ihren Computer neu starten.

So registrieren Sie Intego NetBarrier X4

Öffnen Sie nach dem Neustart Ihres Computers das Programm Intego NetBarrier X4, das sich im Ordner „Programme“ befindet. Intego NetBarrier X4 zeigt dann folgendes Registrierungsfenster an:

Geben Sie in dieses Dialogfeld bitte Ihren Namen, den Namen Ihres Unternehmens (sofern zutreffend) und Ihre Seriennummer ein. Wenn Sie eine verpackte Version gekauft haben, befindet sich die Seriennummer auf einem Aufkleber in der DVD-Hülle. Wenn Sie eine Version aus dem Internet heruntergeladen haben, wurde Ihnen die Seriennummer mit der Bestätigungs-E-Mail zugesendet. Klicken Sie nach Eingabe aller Informationen auf „OK“. Anschließend wird Intego NetBarrier X4 automatisch gestartet. Wenn Sie der Administrator Ihres Computers sind, können Sie die Software konfigurieren.

Da Mac OS X ein Mehrbenutzer-Betriebssystem ist, haben nicht alle Benutzer eines Macintosh die gleichen Privilegien. Nach dem erstmaligen Starten von Intego NetBarrier X4 kann zwar jeder Benutzer die Seriennummer der Software eingeben, aber nur ein Benutzer mit Administratorprivilegien kann Intego NetBarrier X4 konfigurieren.

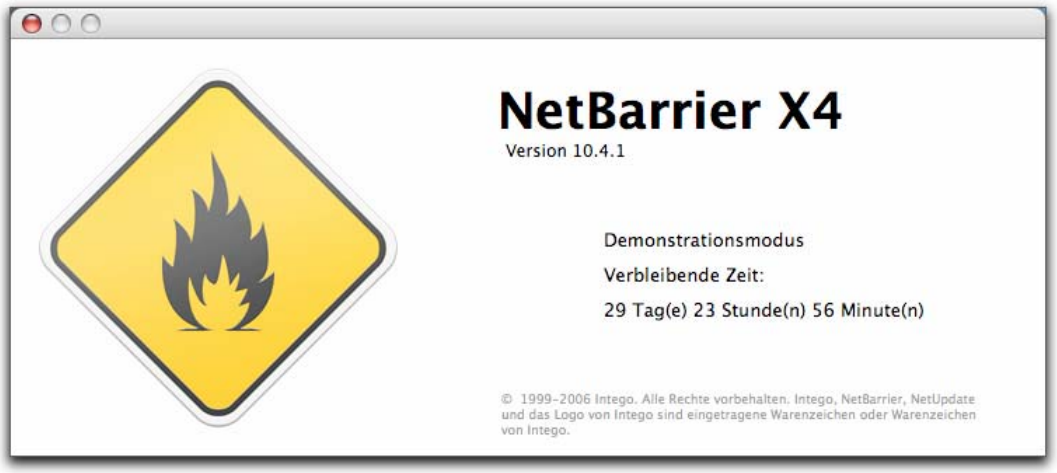
Verwenden von Intego NetBarrier X4 im Demonstrationsmodus

Intego NetBarrier X4 kann maximal 30 Tage lang im Demonstrationsmodus laufen, um Ihnen die Leistungsfähigkeit dieses Programms zu verdeutlichen, bevor Sie es kaufen. Der Demonstrationsmodus von Intego NetBarrier X4 wird aktiviert, indem Sie im Registrierungsfenster, das automatisch angezeigt wird, auf die Schaltfläche „Abbrechen“ klicken.

NetBarrier X4 wird derzeit im Demonstrationsmodus ausgeführt.
Sie können NetBarrier X4 30 Tage lang mit allen Funktionen im Demonstrationsmodus verwenden. Nach Ablauf dieses Zeitraums können Sie auf der Website www.intego.com eine Lizenz für NetBarrier X4 kaufen, um das Programm weiterverwenden zu können.
Seriennummer eingeben...
Demonstrationsmodus

Im Demonstrationsmodus können Sie Intego NetBarrier X4 maximal 30 Tage lang verwenden. Nach Ablauf der Demonstrationsfunktion können Sie Intego NetBarrier X4 entweder kaufen oder Sie müssen das Programm von Ihrem Computer löschen.

Wenn Sie wissen wollen, wie lang Sie Intego NetBarrier X4 noch im Demonstrationsmodus laufen lassen können, müssen Sie die Menüoption „Über NetBarrier X4“ wählen. Im nun geöffneten Fenster sehen Sie, dass die Demonstrationsfunktion von Intego NetBarrier X4 aktiviert ist, und wie viele Tage das Programm noch im Demonstrationsmodus laufen kann.


NetBarrier X4
Version 10.4.1
Demonstrationsmodus
Verbleibende Zeit:
29 Tag(e) 23 Stunde(n) 56 Minute(n)
© 1999–2006 Intego. Alle Rechte vorbehalten. Intego, NetBarrier, NetUpdate und das Logo von Intego sind eingetragene Warenzeichen oder Warenzeichen von Intego.

4 – Erste Schritte

Verwenden von Intego NetBarrier X4

Wenn Sie Intego NetBarrier X4 das erste Mal öffnen, wird Ihnen das Hauptfenster angezeigt.

Verwenden des Hauptfensters von Intego NetBarrier X4

Im Hauptfenster haben Sie Zugriff auf die Funktionen von Intego NetBarrier X4. Hier wird auch eine Zusammenfassung aller Voreinstellungen angezeigt. In diesem Fenster haben Sie also den sofortigen Überblick über alles Wesentliche. In jedem Teil des Hauptfensters werden Informationen über die vier „Verteidigungslinien“ von Intego NetBarrier X4 angezeigt.

Im Abschnitt „Firewall“ des Hauptfensters sehen Sie Informationen über die Firewall sowie das Protokoll und die Einstellungen für den Schutz Ihres Computers vor Trojanischen Pferden.

Im Abschnitt „Vandalismus“ des Hauptfensters sehen Sie Informationen über Ihre Schutzrichtlinien, die Sperrliste, die vertrauenswürdige Gruppe und die Anti-Spyware.

Im Abschnitt „Datenschutz“ des Hauptfensters sehen Sie Informationen über Daten, Banner, Cookies und Filter für das Internetsurfen. Sie erfahren ebenfalls, wann Sie Ihre Cache- und Verlaufsdateien das letzte Mal gelöscht haben. Wenn Sie möchten, können Sie diese Dateien auch in diesem Fenster löschen.

Im Abschnitt „Überwachung“ des Hauptfensters sehen Sie Informationen über ein- und ausgehenden Datenverkehr.

Die beiden anderen Schaltflächen ermöglichen den Zugriff auf andere Funktionen von Intego NetBarrier X4:

Im Abschnitt „NetUpdate“ des Hauptfensters sehen Sie Informationen über die installierte Version von Intego NetBarrier X4, den Zeitpunkt der letzten Prüfung auf eine aktualisierte Version der Software und die Fälligkeit der nächsten Aktualisierung.

Durch Klicken auf die Schaltfläche „Übersicht“ können Sie das Hauptfenster jederzeit wieder öffnen, und zwar unabhängig davon, welches Fenster momentan geöffnet ist.

Im Hauptfenster können Sie durch Klicken auf eine Schaltfläche auf alle Dialogfelder und Registerkarten von Intego NetBarrier X4 zugreifen. Wenn Sie den Mauszeiger über die weißen Etiketten verschieben, werden diese unterstrichen dargestellt. Durch Klicken auf eines dieser Etiketten können Sie das entsprechende Dialogfeld bzw. die entsprechende Registerkarte öffnen.

Klicken Sie auf eine der Schaltflächen links vom Dialogfeld, um wieder diese Dialogfelder zu öffnen. Wenn Sie auf die Schaltfläche „Übersicht“ klicken, wird wieder das Hauptfenster geöffnet.

Verändern der Größe des Fensters von NetBarrier X4

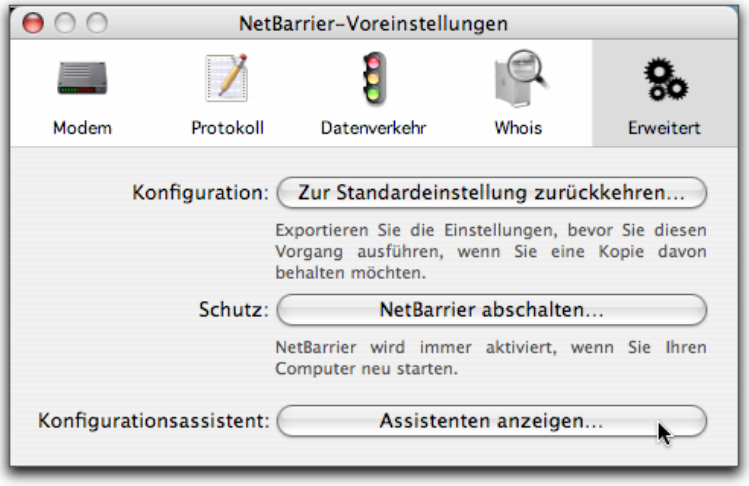
Sie können die Größe jedes Dialogfelds mit Ausnahme des Hauptfensters verändern. Klicken Sie hierzu auf die untere rechte Ecke des Dialogfelds und ziehen Sie die Ecke mit der Maus, bis das Dialogfeld die gewünschte Größe hat.

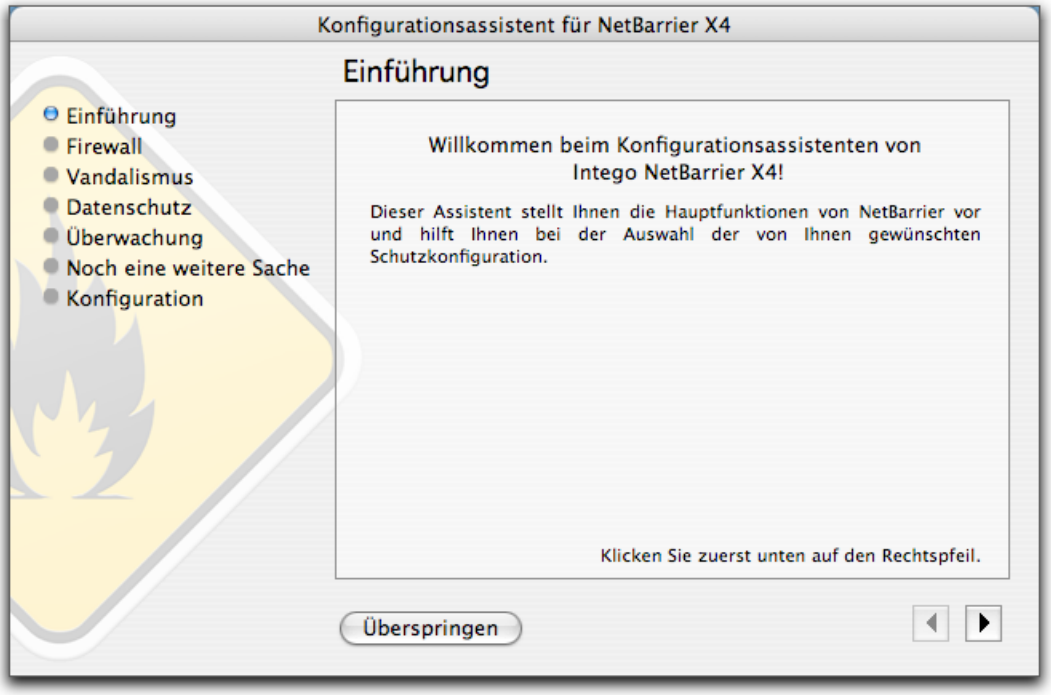
Sie können jedes Fenster verkleinern, indem Sie seine untere rechte Ecke entsprechend verschieben.

Einrichten der Firewall

Wenn Sie Ihren Macintosh nach der Installation von Intego NetBarrier X4 neu starten, beginnt die Software automatisch damit, Ihren Macintosh zu schützen. Die Firewall wird im Client-, lokalen Servermodus aktiviert. Zudem werden alle Aktivitäten im Protokoll aufgezeichnet. In diesem Modus schützt die in Intego NetBarrier X4 integrierte Firewall Ihren Computer, wenn er als Client und Server in einem lokalen Netzwerk fungiert. Ihr Computer kann übers Internet als Client kommunizieren und in einem lokalen Netzwerk sowohl als Client als auch als Server fungieren. Weitere Informationen über die Firewall-Modi von NetBarrier X4 erhalten Sie weiter vorn in diesem Handbuch.

Intego NetBarrier X4 enthält einen Konfigurationsassistenten, mit dem Sie die Basiskonfiguration der Software schnell und einfach durchführen können. So passen Sie das Programm an Ihre Art des Netzwerkeinsatzes an. Wenn Sie NetBarrier X4 zum ersten Mal öffnen, wird der Konfigurationsassistent automatisch gestartet. Wenn Sie von einer vorherigen Version von NetBarrier aktualisieren, müssen Sie den Konfigurationsassistenten selbst starten. Wählen Sie hierzu im Menü von NetBarrier X4 „NetBarrier X4-Voreinstellungen“ > „Erweitert“. Klicken Sie anschließend auf „Assistenten anzeigen…“ am unteren Fensterrand. Um den Konfigurationsassistenten ausführen zu können, benötigen Sie ein Administratorkennwort.





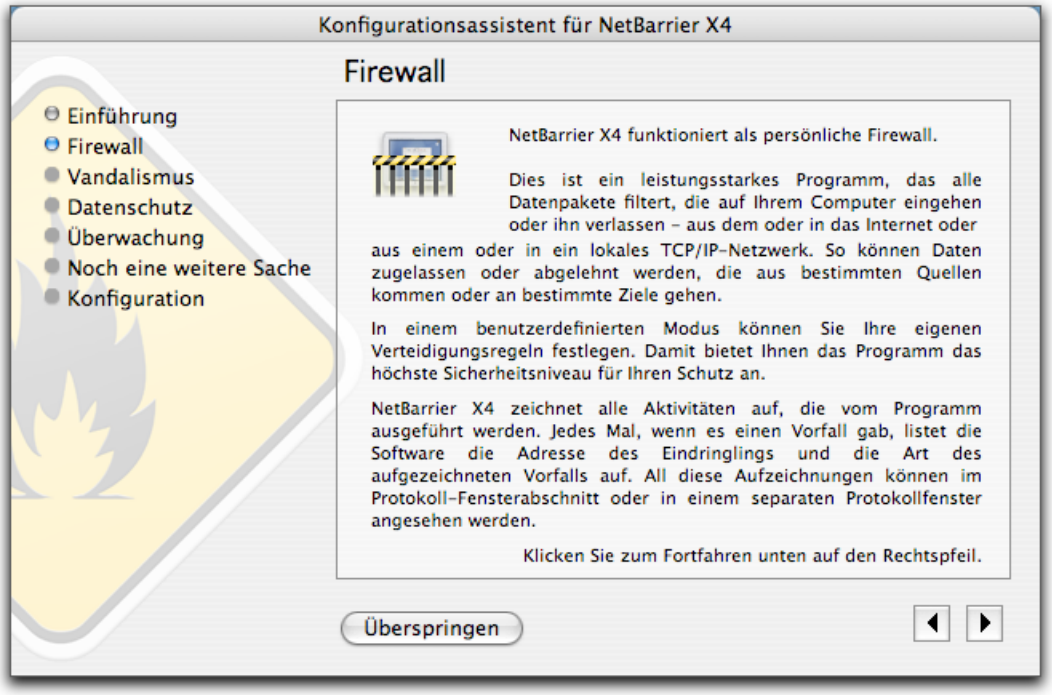
Der Konfigurationsassistent von Intego NetBarrier X4 führt Sie durch eine Kurzanleitung der verschiedenen Funktionen und unterstützt Sie bei der Einrichtung des Programms:

- **Firewall**
- **Vandalismus**
- **Datenschutz**
- **Überwachung**
- **Noch eine weitere Sache**
- **Konfiguration**

Klicken Sie auf den nach rechts weisenden Pfeil, um mit der Konfiguration von Intego NetBarrier X4 zu beginnen. Klicken Sie auf den nach links weisenden Pfeil, um wieder die vorigen Dialogfelder zu öffnen.

Sie können auch auf die Schaltfläche „Abbrechen“ klicken, wenn Sie den Konfigurationsassistenten nicht verwenden möchten.

In den ersten vier Fenstern erhalten Sie im Anschluss an die Einführung Informationen über jede der vier Verteidigungslinien von Intego NetBarrier X4.


Konfigurationsassistent für NetBarrier X4
Einführung
Firewall
Vandalismus
Datenschutz
Überwachung
Noch eine weitere Sache
Konfiguration
Firewall
NetBarrier X4 funktioniert als persönliche Firewall.
Dies ist ein leistungsstarkes Programm, das alle Datenpakete filtert, die auf Ihrem Computer eingehen oder ihn verlassen – aus dem oder in das Internet oder aus einem oder in ein lokales TCP/IP-Netzwerk. So können Daten zugelassen oder abgelehnt werden, die aus bestimmten Quellen kommen oder an bestimmte Ziele gehen.
In einem benutzerdefinierten Modus können Sie Ihre eigenen Verteidigungsregeln festlegen. Damit bietet Ihnen das Programm das höchste Sicherheitsniveau für Ihren Schutz an.
NetBarrier X4 zeichnet alle Aktivitäten auf, die vom Programm ausgeführt werden. Jedes Mal, wenn es einen Vorfall gab, listet die Software die Adresse des Eindringlings und die Art des aufgezeichneten Vorfalls auf. All diese Aufzeichnungen können im Protokoll-Fensterabschnitt oder in einem separaten Protokollfenster angesehen werden.
Klicken Sie zum Fortfahren unten auf den Rechtspfeil.
Überspringen

Weitere Informationen über die zusätzlichen Funktionen von NetBarrier X4 erhalten Sie im Fenster „Noch eine weitere Sache…“.

Im Konfigurationsfenster können Sie auswählen, welche Konfiguration von NetBarrier X4 Sie verwenden möchten.

Standard

Wenn Sie diese Sicherheitsstufe auswählen, befindet sich die Firewall von Intego NetBarrier X4 im Client-, lokalen Servermodus. Das Programm schützt Ihren Computer, wenn er als Client und lokaler Netzwerkserver fungiert. Ihr Computer kann übers Internet als Client kommunizieren und in einem lokalen Netzwerk sowohl als Client als auch als Server fungieren. Alle Antivandalismus- und Datenschutzfilter sind deaktiviert. Diese Konfiguration eignet sich für Benutzer, die einen Netzwerkzugriff auf ihren Computer zulassen müssen.

Normal

Wenn Sie diese Sicherheitsstufe auswählen, befindet sich die Firewall von Intego NetBarrier X4 ausschließlich im Client-Modus. Das Programm schützt Ihren Computer, wenn er nur als Client in einem lokalen Netzwerk fungiert oder

wenn er mit dem Internet verbunden ist. Die Server-Funktionen Ihres Computers sind gesperrt. Alle Antivandalismus- und Datenschutzfilter sind deaktiviert. Diese Konfiguration ist an die Bedürfnisse der meisten Benutzer angepasst, die ihren Computer nicht als Netzwerkserver verwenden.

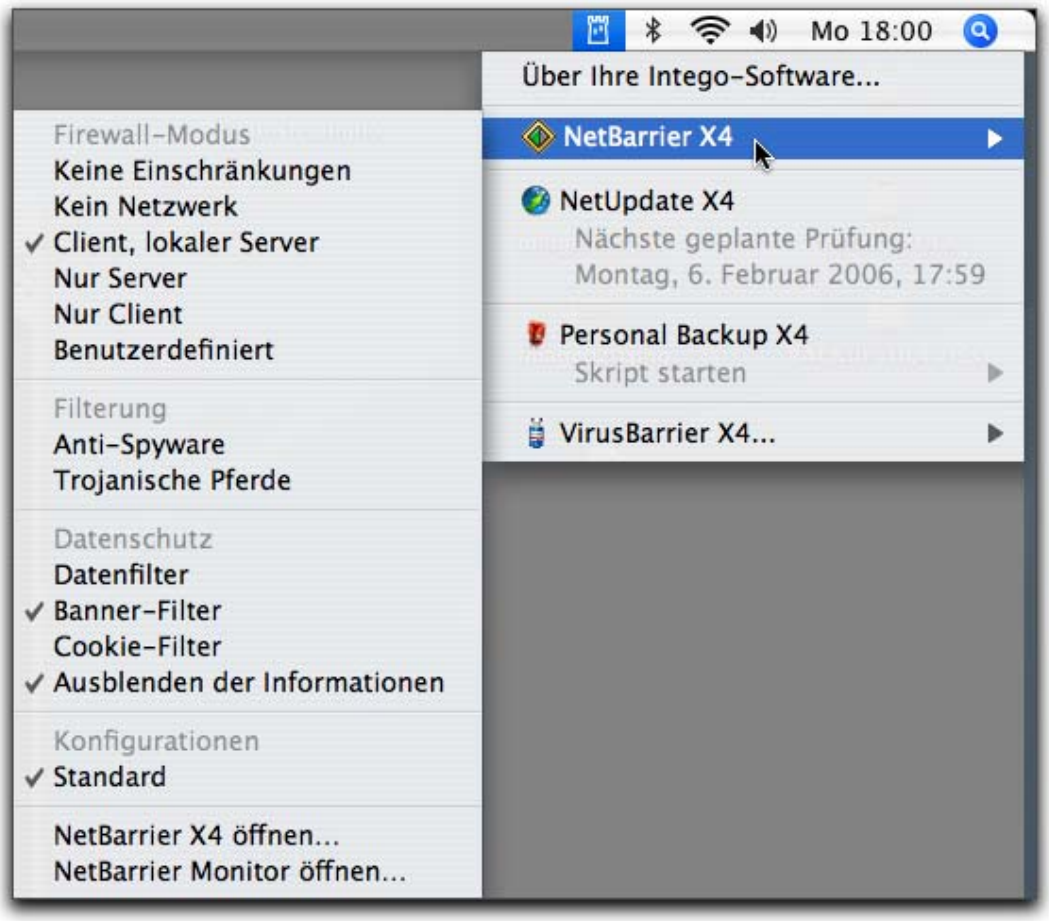
Stark

Wenn Sie diese Sicherheitsstufe auswählen, befindet sich die Firewall von Intego NetBarrier X4 ausschließlich im Client-Modus. Das Programm schützt Ihren Computer, wenn er nur als Client in einem lokalen Netzwerk fungiert oder wenn er mit dem Internet verbunden ist. Die Server-Funktionen Ihres Computers sind gesperrt. Alle Antivandalismus- und Datenschutzfilter sind aktiviert. Diese Konfiguration wird Benutzern empfohlen, die einen maximalen Schutz wünschen. Beachten Sie bitte, dass Sie mit der Auswahl dieser Konfiguration bestimmte Arten des Datenverkehrs sperren, die Sie nicht notwendigerweise sperren möchten.

Klicken Sie zur Aktivierung der von Ihnen ausgewählten Konfiguration auf die Schaltfläche „Konfigurieren“.

Verwenden des Menüs von NetBarrier X4

Mit den Softwareprogrammen von Intego wird ein Menü in Ihrer Menüzeile installiert, über das Sie einen schnellen Zugriff auf viele Funktionen der auf Ihrem Computer installierten Intego-Software erhalten. (Sie können dieses Menü in den Voreinstellungen von Intego NetUpdate X4 abschalten; weitere Informationen hierzu erhalten Sie im Benutzerhandbuch von NetUpdate X4). Klicken Sie aufs Symbol von Intego NetBarrier X4 in der Menüleiste, um das Menü anzeigen zu lassen.



In diesem Menü können Sie einen von sechs Firewall-Modi auswählen. Hierbei ändert sich das Menüsymbol, um den gewählten Firewall-Modus anzuzeigen.

Keine Einschränkungen

Kein Netzwerk

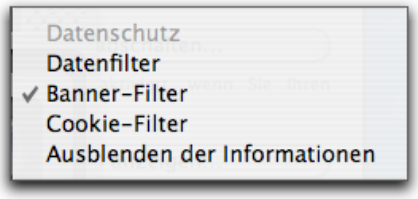
Client, lokaler Server

Nur Server

Nur Client

Benutzerdefiniert

In diesem Menü können Sie auch Funktionen von Intego NetBarrier X4 abschalten. Durch eine Markierung im Menü wird angezeigt, welche Funktion aktiviert ist. Wenn Sie beispielsweise den Bannerfilter aktivieren wollen, müssen Sie diese Option im Menü auswählen. Eine Markierung wird eingeblendet, die Ihnen anzeigt, dass diese Funktion aktiviert ist.



Aus dem Menü von Intego NetBarrier X4 können Sie auch komplette Konfigurationen wählen. Weitere Informationen über das Verwenden von Konfigurationssätzen finden Sie im Kapitel 6, **Voreinstellungen und Konfigurationen**.

Sie können NetBarrier X4 oder den Monitor auch von diesem Menü aus öffnen, indem Sie „NetBarrier X4 öffnen…“ oder „NetBarrier Monitor öffnen…“ auswählen.

Intego Widgets

Wenn Sie NetBarrier X4 installieren, werden zugleich zwei Widgets für Intego installiert. Im ersten Widget wird Ihnen der Status von NetBarrier X4 sowie die gesamte weitere Intego-Software angezeigt, die eventuell gerade auf Ihrem Computer ausgeführt wird - beispielsweise Intego Personal Backup X4 oder VirusBarrier X4.

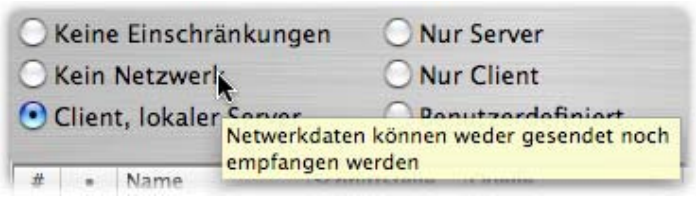
Beim zweiten Intego-Widget handelt es sich um das Widget für NetUpdate. Damit können Sie einfach überprüfen, ob derzeit Aktualisierungen für Ihre Intego-Software zur Verfügung stehen. Es sieht folgendermaßen aus:

Passwortschutz von Intego NetBarrier X4

Intego NetBarrier X4 verwendet den in Mac OS X integrierten Passwortschutz. Sie können das Programm nur installieren und konfigurieren, wenn Sie Administratorprivilegien haben und sich mit einer entsprechenden Benutzerkennung und einem Passwort bei Ihrem Computer anmelden. Benutzer, die nicht über Administratorprivilegien verfügen, können die Einstellungen von Intego NetBarrier X4 nicht verändern. Diese Benutzer können zwar Protokolle und grafische Messskalen zur Anzeige der Netzwerkaktivitäten einsehen, aber keine Änderungen an Intego NetBarrier X4 vornehmen.

Aufrufen von Hilfeinformationen

Sie können Hilfeinformationen über einige Funktionen von Intego NetBarrier X4 aufrufen, indem Sie den Mauszeiger über den entsprechenden Bereich verschieben:



Nun erscheint eine so genannte QuickInfo zur Erklärung der entsprechenden Funktion.

Links zur Website von Intego

Im Menü von NetBarrier X4 stehen Ihnen die folgenden beiden Links zur Verfügung: „Intego-Website besuchen“ und „NetBarrier registrieren“. Über den ersten Link gelangen Sie auf die Homepage der Intego-Website. Über den zweiten Link gelangen Sie auf die Registrierungsseite, auf der Sie Ihre Software und Ihre Seriennummer registrieren lassen können.

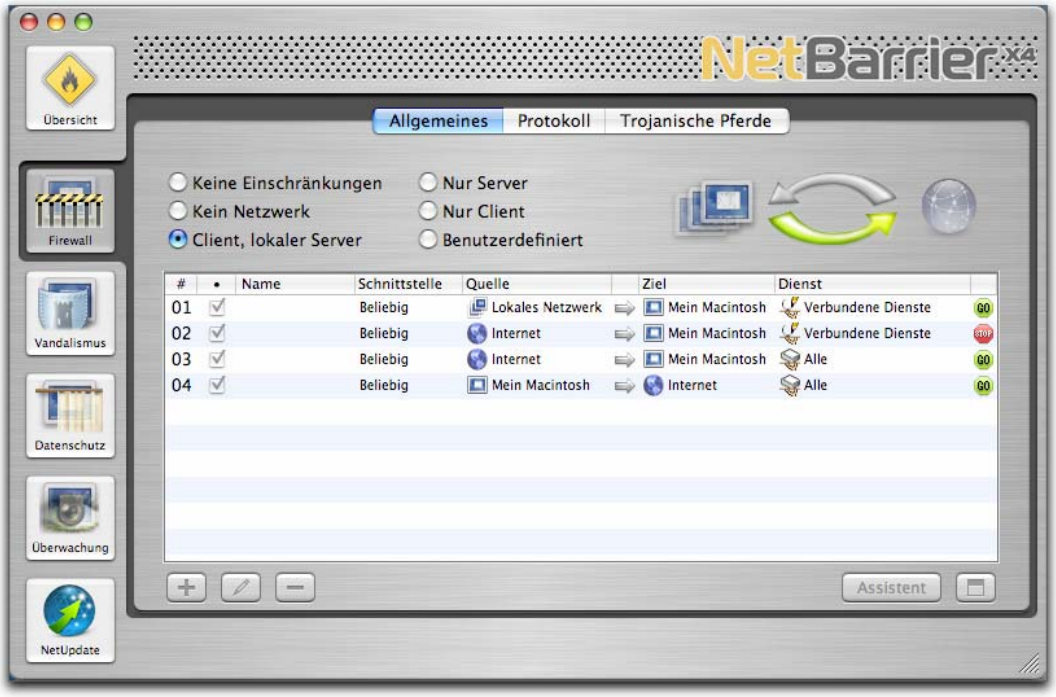
5 – Die vier Verteidigungslinien

Intego NetBarrier X4 ist ein leistungsfähiges und einfach anzuwendendes Programm zum Schutz Ihres Computers bei Verbindung mit einem Netzwerk. Das Programm bietet vier „Verteidigungslinien“, um Ihren Computer vor Eindringversuchen und Angriffen zu schützen.

Firewall

Intego NetBarrier X4 enthält eine persönliche Firewall Die Firewall filtert alle Datenpakete, die von Ihrem Computer aus einem lokalen TCP/IP-Netzwerk oder dem Internet empfangen und über dieses versandt werden, sodass nur Daten von zugelassenen Datenquellen empfangen und an zugelassene Datenziele versandt werden können. Die Firewall schützt Ihren Computer auch vor Trojanischen Pferden, indem die von diesen verwendeten Ports gesperrt werden.

Das Dialogfeld „Firewall“ kann durch Klicken aufs Symbol Firewall links im Hauptfenster geöffnet werden. Nun erscheint das Fenster „Firewall“ mit seinen drei Registerkarten: Allgemeines, Protokoll und Trojanische Pferde.



Firewall-Einstellungen

Die in Intego NetBarrier X4 integrierte Firewall kann durch 6 verschiedene Einstellungen an die persönlichen Anforderungen des Benutzers angepasst werden. Die fünf ersten Einstellungen, die auf vorprogrammierten Regeln basieren, decken alle normalen Situationen ab. Die letzte Einstellung, **Benutzerdefiniert**, ermöglicht es Ihnen, eigene Regeln zu definieren, um exakt festzulegen, wer auf Ihren Computer zugreifen darf und welche Daten von Ihrem Computer versandt werden dürfen.

Keine Einschränkungen

In diesem Modus gibt es keine Einschränkungen: die in Intego NetBarrier X4 integrierte Firewall filtert und sperrt keinerlei ein- und ausgehende Daten. Mit dieser Option können Sie die Firewall abschalten.

Kein Netzwerk

In diesem Modus sperrt die in Intego NetBarrier X4 integrierte Firewall den Empfang und den Versand sämtlicher Daten aus einem und in ein lokales TCP/IP-Netzwerk bzw. aus dem/ins Internet. Dieser Modus ermöglicht es Ihnen, jeden Netzwerk-Datenverkehr Ihres Computers zu sperren, wenn Sie beispielsweise von Ihrem Computer abwesend sind.

Client, lokaler Server

In diesem Modus schützt die in Intego NetBarrier X4 integrierte Firewall Ihren Computer, wenn er als Client und Server in einem lokalen Netzwerk fungiert. Ihr Computer kann übers Internet als Client kommunizieren und in einem lokalen Netzwerk sowohl als Client als auch als Server fungieren.

Nur Server

In diesem Modus schützt die in Intego NetBarrier X4 integrierte Firewall Ihren Computer, wenn er nur als Server in einem lokalen Netzwerk fungiert. Die Client-Funktionen Ihres Computers sind gesperrt.

Nur Client

In diesem Modus schützt die in Intego NetBarrier X4 integrierte Firewall Ihren Computer, wenn er nur als Client in einem lokalen Netzwerk fungiert oder wenn er mit dem Internet verbunden ist. Die Server-Funktionen Ihres Computers sind gesperrt.

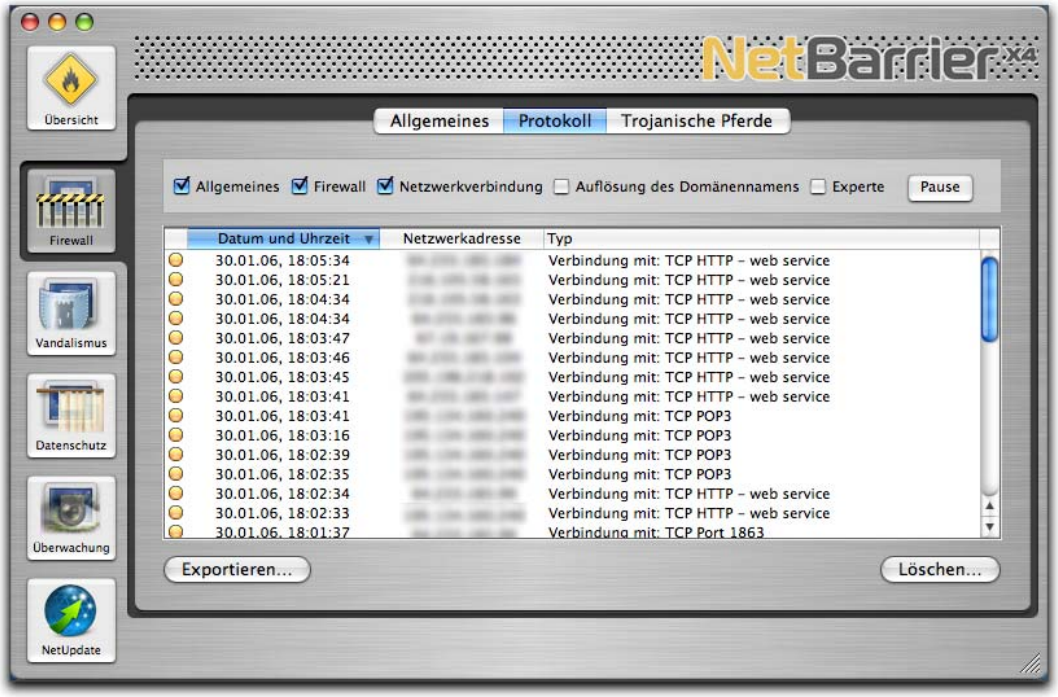
Benutzerdefiniert

Diese Option ermöglicht es Ihnen, Ihre eigenen Filterregeln für die in Intego NetBarrier X4 integrierte Firewall zu definieren. Da Sie aber mit dieser Einstellung Zugriff auf die leistungsstarken Möglichkeiten zum Erstellen von Regeln erhalten, für die Sie Kenntnisse über Netzwerke und Protokolle benötigen, sollte diese Option nur von Computerbenutzern verwendet werden, die wissen, was die verschiedenen Parameter bedeuten. Weitere Informationen über den Modus „Benutzerdefiniert“ enthält das Kapitel 7, **Individuell konfigurierter Schutz**.

Protokoll

Funktion des Protokolls

Im Protokoll werden alle Internet-Aktivitäten des Benutzers Ihres Computers aufgezeichnet. Im Protokoll werden alle Ereignisse, die Internet-Adressen etwaiger Eindringlinge und die Art jedes Ereignisses aufgezeichnet.


NetBarrier X4
Übersicht
Firewall
Vandalismus
Datenschutz
Überwachung
NetUpdate
Allgemeines
Protokoll
Trojanische Pferde
Allgemeines
Firewall
Netzwerkverbindung
Auflösung des Domänennamens
Experte
Pause
Datum und Uhrzeit
Netzwerkadresse
Typ
30.01.06, 18:05:34 Verbindung mit: TCP HTTP – web service
30.01.06, 18:05:21 Verbindung mit: TCP HTTP – web service
30.01.06, 18:04:34 Verbindung mit: TCP HTTP – web service
30.01.06, 18:04:34 Verbindung mit: TCP HTTP – web service
30.01.06, 18:03:47 Verbindung mit: TCP HTTP – web service
30.01.06, 18:03:46 Verbindung mit: TCP HTTP – web service
30.01.06, 18:03:45 Verbindung mit: TCP HTTP – web service
30.01.06, 18:03:41 Verbindung mit: TCP HTTP – web service
30.01.06, 18:03:41 Verbindung mit: TCP POP3
30.01.06, 18:03:16 Verbindung mit: TCP POP3
30.01.06, 18:02:39 Verbindung mit: TCP POP3
30.01.06, 18:02:35 Verbindung mit: TCP POP3
30.01.06, 18:02:34 Verbindung mit: TCP HTTP – web service
30.01.06, 18:02:33 Verbindung mit: TCP HTTP – web service
30.01.06, 18:01:37 Verbindung mit: TCP Port 1863
Exportieren...
Löschen...

Auswahl der im Protokoll anzuzeigenden Informationen

Sie können festlegen, welche Informationen im Protokoll angezeigt werden sollen. Durch Markieren eines der nachstehend angegebenen Kontrollkästchen können Sie die entsprechende Aktivität überwachen. Wenn eines dieser Kontrollkästchen nicht markiert ist, kann die entsprechende Aktivität nicht überwacht werden.

Allgemeines

Dies sind generelle Aktivitäten von Intego NetBarrier X4 wie das Starten des Programms und die Ausgabe von Warnmeldungen.

Firewall

Intego NetBarrier X4 protokolliert alle Firewall-Aktivitäten, wenn Firewall-Regeln angewandt werden. Voraussetzung hierfür ist, dass die Protokollierung in den Regeln aktiviert wurde.

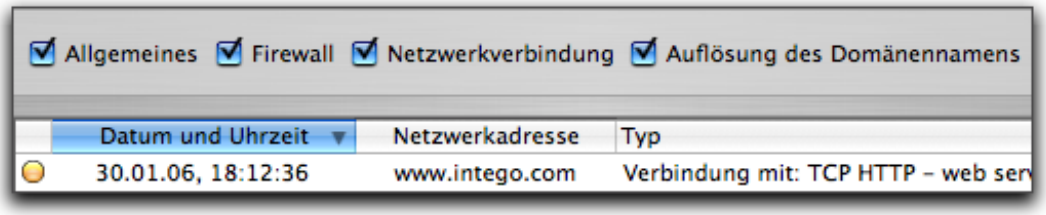
Netzwerkverbindung

Intego NetBarrier X4 protokolliert alle Verbindungen mit Netzwerken oder dem Internet, und wenn Computer mit gesperrten IP-Adressen versuchen, eine Verbindung mit Ihrem Computer herzustellen.

Auflösung von Domänennamen

Intego NetBarrier X4 ermöglicht es Ihnen, Eindringlinge zu verfolgen, indem Sie die Domänennamen anderer Computer auflösen. Internet-Adressen kommen in zwei unterschiedlichen Formaten vor: Internet-Adressen haben zwei unterschiedliche Formate: IP-Nummern wie z.B. 255.255.0.0 und Domänennamen wie intego.com. Die Beziehung zwischen IP-Nummern und Domänennamen wird von speziellen Servern (DNS, Domain Name Servers = Domänennamenserver) im gesamten Internet verwaltet.

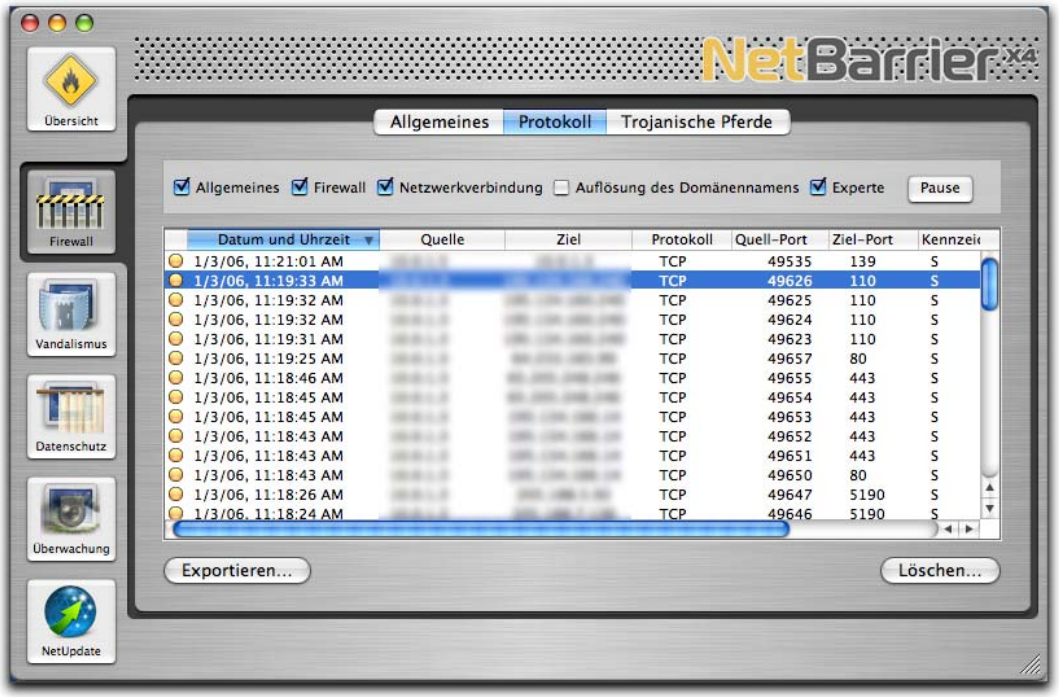
Wenn das Kontrollkästchen „Auflösung des Domänennamens“ auf der Registerkarte „Protokoll“ markiert ist, versucht Intego NetBarrier X4, die Domänennamen aller im Protokoll enthaltenen IP-Nummern aufzulösen. Wenn ein Domänenname gefunden wurde, wird er anstelle der IP-Nummer angezeigt.



Anmerkung: Gelegentlich ist Intego NetBarrier X4 nicht in der Lage, die Namen einiger Internetadressen aufzulösen, da nicht all diesen Adressen Domänennamen zugeordnet sind.

Expertenmodus

Wenn Sie festgelegt haben, dass das Protokoll im Expertenmodus angezeigt werden soll, erscheinen in diesem zusätzliche Spalten. Diese Spalten sind mit Quelle, Protokoll, Quell-Port, Ziel-Port, Kennzeichen, Schnittstelle und Art beschriftet.

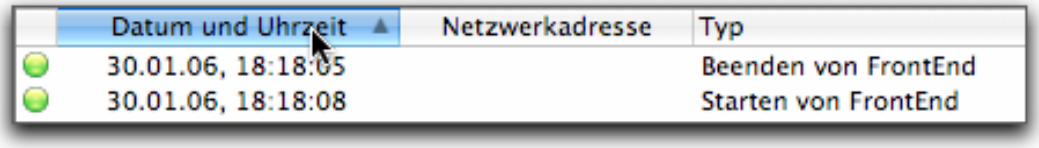


Pausieren der kontinuierlichen Protokollanzeige

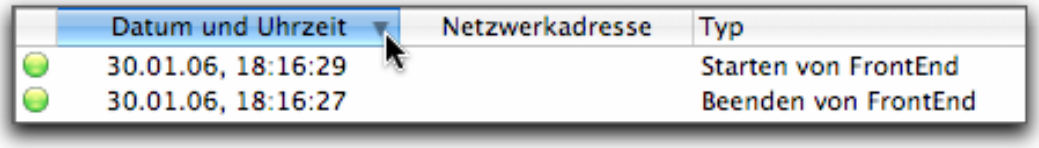
Wenn innerhalb kurzer Zeit viele Verbindungen mit Ihrem Computer hergestellt und beendet werden, kann es problematisch sein, das sich ständig aktualisierende Protokoll zu lesen. Sie können das Aktualisieren des Protokolls abschalten, indem Sie auf die Schaltfläche „Pause“ klicken. Das Protokoll wird angehalten, damit Sie die Daten lesen können. Das Protokoll zeichnet jedoch weiterhin Daten auf und zeigt diese an, wenn Sie das Protokoll weiterlaufen lassen. Klicken Sie erneut auf die Schaltfläche „Pause“, um wieder die Echtzeitanzeige des Protokolls zu aktivieren.

Ändern der Protokollanzeige

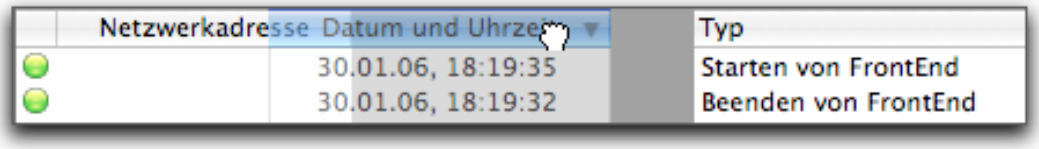
Sie können die Einträge im Protokoll nach den Spalteninhalten sortieren lassen, indem Sie auf die gewünschte Spaltenüberschrift klicken.



Sie können das Protokoll auch in auf- oder absteigender Reihenfolge sortieren lassen. Klicken Sie hierzu entweder noch einmal auf die Spaltenüberschrift oder klicken Sie auf die Schaltfläche „Sortieren“ – dies ist das kleine Dreieck in der zum Sortieren ausgewählten Spaltenüberschrift.

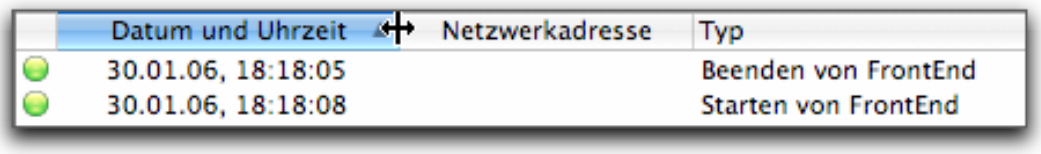


Sie können auch die Reihenfolge der Spalten ändern. Klicken Sie hierzu in die Überschrift der gewünschten Spalte, halten Sie die Maustaste gedrückt und ziehen Sie die Überschrift in die gewünschte Position. Lassen Sie die Maustaste wieder los.



Sie können die Breite jeder Spalte des Protokolls ändern. Verschieben Sie hierzu den Mauszeiger über die vertikale Linie zwischen den beiden Spalten. Der Mauszeiger verändert nun seine Form, wodurch angezeigt wird, dass Sie die vertikale Trennlinie

verschieben können. Klicken Sie auf die vertikale Trennlinie und verschieben Sie diese nach links oder rechts, um die Spaltenbreite zu verändern.



Wenn Sie die Anzeige der Liste vergrößern möchten, klicken Sie auf die untere rechte Ecke des Dialogfelds, halten Sie die Maustaste gedrückt und ziehen Sie die Ecke mit der Maus, bis das Dialogfeld die gewünschte Größe hat.

Inhalt des Protokolls

Jeder Protokolleintrag enthält 4 Elemente:

Symbole

Das grüne Symbol zeigt allgemeine Aktivitäten an.

Das gelbe Symbol zeigt Firewall-Aktivitäten an.

Das rote Symbol zeigt Netzwerkaktivitäten an.

Datum und Uhrzeit

Der Zeitpunkt (Datum und Uhrzeit), zu dem das Ereignis stattfand.

Netzwerkadresse

Die IP-Nummer des Computers, der die Verbindung herstellte. Wenn Sie das Kontrollkästchen „Auflösung des Domänennamens“ markiert haben, sehen Sie die Domänennamen der Computer, die Intego NetBarrier X4 auf der Basis der zugehörigen IP-Nummern ermitteln konnte.

Typ

Dies ist die Art des protokollierten Ereignisses.

Wenn Sie sich den Inhalt des Protokolls im Expertenmodus anzeigen lassen, werden detailliertere Informationen angezeigt:

Symbole

Das grüne Symbol zeigt allgemeine Aktivitäten an.

Das gelbe Symbol zeigt Firewall-Aktivitäten an.

Das rote Symbol zeigt Netzwerkaktivitäten an.

Datum und Uhrzeit

Der Zeitpunkt (Datum und Uhrzeit), zu dem das Ereignis stattfand.

Quelle

Die IP-Nummer des Computers, der die Verbindung herstellte.

Ziel

Die IP-Adresse, an die die Daten bei diesem Vorfall gesendet wurden. Wenn Sie das Kontrollkästchen „Auflösung des Domänennamens“ markiert haben, sehen Sie die Domänennamen der Computer, die Intego NetBarrier X4 auf der Basis der zugehörigen IP-Nummern ermitteln konnte.

Protokoll

TCP, UDP, ICMP und IGMP.

Quell-Port

Der Port, über den die Daten gesendet werden.

Ziel-Port

Der Port, über den die Daten empfangen werden.

Kennzeichen

Hier werden die folgenden TCP-Kennzeichen angezeigt: A (Acknowledge = quittieren), S (Synchronize sequence number = Synchronisationsfolgenummer), F (end of data = Ende der Daten) und R (Reset = zurücksetzen).

Schnittstelle

Dies ist die Netzwerkschnittstelle, worüber die Daten gesendet werden. Wenn Ihr Computer über mehrere Netzwerkschnittstellen verfügt (z.B. einen Ethernet-Anschluss und eine AirPort-Karte), wird hiermit die Netzwerkschnittstelle

angegeben. Wenn in Ihren Computer nur eine Netzwerkschnittstelle eingebaut ist, werden in dieser Spalte stets die gleichen Informationen angezeigt.

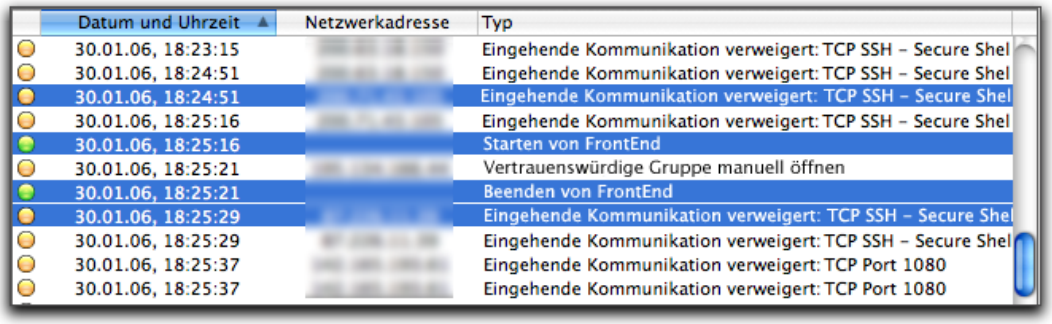
Typ
Dies ist die Art des protokollierten Ereignisses.

Löschen des Protokolls

Um alle im Protokoll enthaltenen Informationen zu löschen, müssen Sie nur auf die Schaltfläche „Löschen…“ klicken. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie das Protokoll wirklich löschen wollen. Klicken Sie auf die Schaltfläche „Löschen…“, um das Protokoll zu löschen, oder auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Auswählen der Protokolldaten

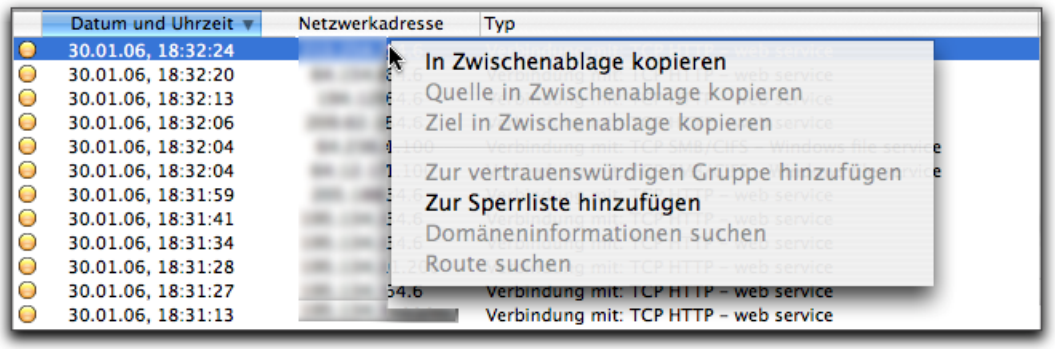
Sie können Protokolldaten in die Zwischenablage kopieren, aus dieser in ein Dokument eines anderen Programms einsetzen oder in ein anderes Fenster ziehen. Sie können mehrere benachbarte Elemente eines Protokolls gleichzeitig auswählen. Klicken Sie hierzu aufs gewünschte Objekt, halten Sie die Umschalttaste gedrückt und wählen Sie die anderen Elemente. Alle Zeilen zwischen der ersten und der letzten werden nun hervorgehoben dargestellt. Wenn Sie mehrere nicht benachbarte Elemente auswählen wollen, müssen Sie die Befehlstaste gedrückt halten und die Elemente wählen.


Datum und Uhrzeit
Netzwerkadresse
Typ
30.01.06, 18:23:15 Eingehende Kommunikation verweigert: TCP SSH – Secure Shel
30.01.06, 18:24:51 Eingehende Kommunikation verweigert: TCP SSH – Secure Shel
30.01.06, 18:24:51 Eingehende Kommunikation verweigert: TCP SSH – Secure Shel
30.01.06, 18:25:16 Eingehende Kommunikation verweigert: TCP SSH – Secure Shel
30.01.06, 18:25:16 Starten von FrontEnd
30.01.06, 18:25:21 Vertrauenswürdige Gruppe manuell öffnen
30.01.06, 18:25:21 Beenden von FrontEnd
30.01.06, 18:25:29 Eingehende Kommunikation verweigert: TCP SSH – Secure Shel
30.01.06, 18:25:29 Eingehende Kommunikation verweigert: TCP SSH – Secure Shel
30.01.06, 18:25:37 Eingehende Kommunikation verweigert: TCP Port 1080
30.01.06, 18:25:37 Eingehende Kommunikation verweigert: TCP Port 1080

Nach der Auswahl der gewünschten Protokolldaten können Sie diese in die Zwischenablage kopieren, aus dieser in ein Dokument eines anderen Programms einsetzen oder in ein anderes Fenster bzw. auf den Schreibtisch ziehen.

Kontextmenü des Protokollfensters

Wenn Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh auf einen Protokolleintrag klicken, wird ein Kontextmenü geöffnet.



Dieses Menü ermöglicht Ihnen Folgendes:

In Zwischenablage kopieren

Mit der Option „In Zwischenablage kopieren“ im Kontextmenü können Sie den Inhalt der entsprechenden Zeile in die Zwischenablage kopieren. Anschließend können Sie den Inhalt der Zwischenablage in ein Dokument jedes beliebigen Anwendungsprogramms einsetzen.

Zur vertrauenswürdigen Gruppe hinzufügen

Mit dieser Option im Kontextmenü können Sie die IP-Adresse des ausgewählten Objekts in die vertrauenswürdige Gruppe verschieben. Weitere Informationen über die vertrauenswürdige Gruppe finden Sie im Unterabschnitt **Vertrauenswürdige Gruppe** weiter unten in diesem Kapitel.

Zur Sperrliste hinzufügen

Mit dieser Option im Kontextmenü können Sie die IP-Adresse des ausgewählten Objekts in die Sperrliste verschieben. Weitere Informationen über die Sperrliste finden Sie im Unterabschnitt **Sperrliste** weiter unten in diesem Kapitel.

Domäneninformationen suchen

Mit dieser Option im Kontextmenü können Sie Intego NetBarrier X4 den Domänennamen oder die IP-Adresse unter Verwendung der integrierten Whois-Funktion suchen lassen. Weitere Informationen über Whois finden Sie im Unterabschnitt **Whois** weiter unten in diesem Kapitel.

Route suchen

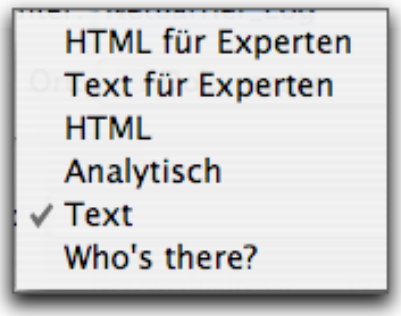
Mit dieser Option im Kontextmenü können Sie die Registerkarte „Routenverfolgung“ öffnen. Nun wird der Datenweg zwischen Ihrem Computer und dem Computer mit der IP-Adresse im Protokoll zurückverfolgt.

Exportieren des Protokolls

Sie können das Protokoll in mehreren Formaten exportieren. Beim manuellen Exportieren werden nur die angezeigten Daten exportiert. Wenn Sie also beispielsweise nur das Kontrollkästchen „Firewall“ auf der Registerkarte „Protokoll“ markiert haben, werden nur die Firewall-Daten exportiert. (Sie können die Protokolldaten auch automatisch exportieren lassen. Weitere Informationen hierzu finden Sie im Kapitel 6, **Einstellungen für Protokollexport**.)

Sie können das Protokoll exportieren, indem Sie auf die Schaltfläche „Exportieren…“ klicken. Nun wird ein Dialogfeld geöffnet, sodass Sie die Datei speichern können. Hierbei können Sie den Namen der Datei ändern. Wählen Sie den Ort, an dem das Protokoll gespeichert werden sollen. Standardmäßig werden alle Dateien mit exportierten Daten im Ordner „Eigene Dateien“ des angemeldeten Benutzers gespeichert.

Protokolle können in sechs Formaten exportiert werden: Klicken Sie ins Popup-Menü „Format“, um das Exportformat zu wählen.



Sie haben die Auswahl aus folgenden Formaten:

HTML für Experten

Hierbei handelt es sich ums HTML-Format mit zusätzlichen Spalten. In diesem Format werden die gleichen Informationen wie im Expertenmodus angezeigt.

Text für Experten

Hierbei handelt es sich ums Textformat mit zusätzlichen Spalten. In diesem Format werden die gleichen Informationen wie im Expertenmodus angezeigt. Die Spalten werden durch Reiter separiert und können auf einfachste Weise in ein Arbeitsblatt eines Tabellenkalkulationsprogramms wie z.B. Microsoft Excel importiert werden.

HTML

Wenn Sie das Protokoll als HTML-Datei speichern, können Sie es mit jedem Webbrowser öffnen. Das Protokoll wird in Tabellenform angezeigt.

Analytisch

Dieses Format ähnelt dem Format „Text für Experten“, wobei allerdings keine Reiter vorhanden sind. Manche Felder sind beschriftet.

Text

Im Textformat exportierte Protokolle können mit jedem Textverarbeitungsprogramm verarbeitet werden.

Who’s there?

Ein in diesem (Text-)Format exportiertes Protokoll enthält folgende Informationen:

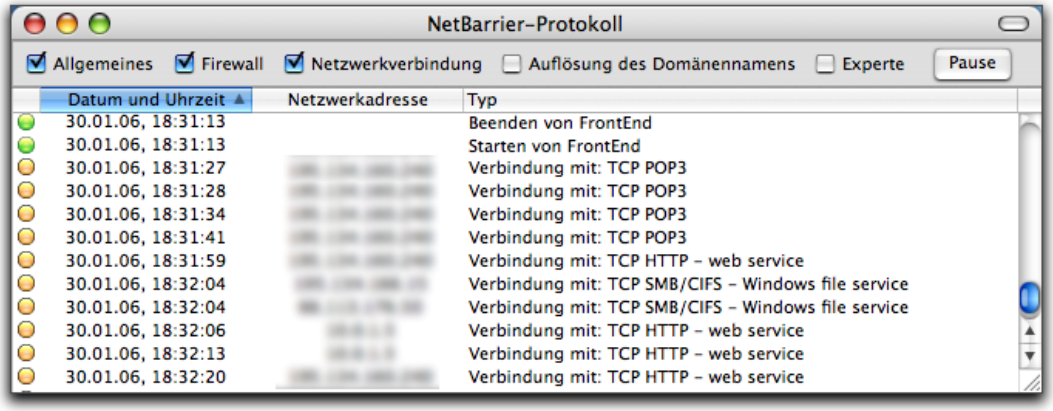
DATUM:	Datum der Verbindungsherstellung.
ZEIT:	Uhrzeit der Verbindungsherstellung.

ERGEBNIS:	Ergebnis der Verbindung.
HOSTNAME:	Die IP-Adresse des Servers.
SERVER_PORT:	Der für diese Verbindung verwendete Server-Port.
VERFAHREN:	Das verwendete Übertragungsprotokoll (TCP oder UDP).

Klicken Sie auf die Schaltfläche „Sichern“. Nun verfügen Sie über eine Kopie Ihres Protokolls, die Sie mit einem beliebigen Textverarbeitungsprogramm (Textformat), Tabellenkalkulationsprogramm (Textformat) oder Webbrowser (HTML) öffnen können.

Öffnen des Protokollfensters

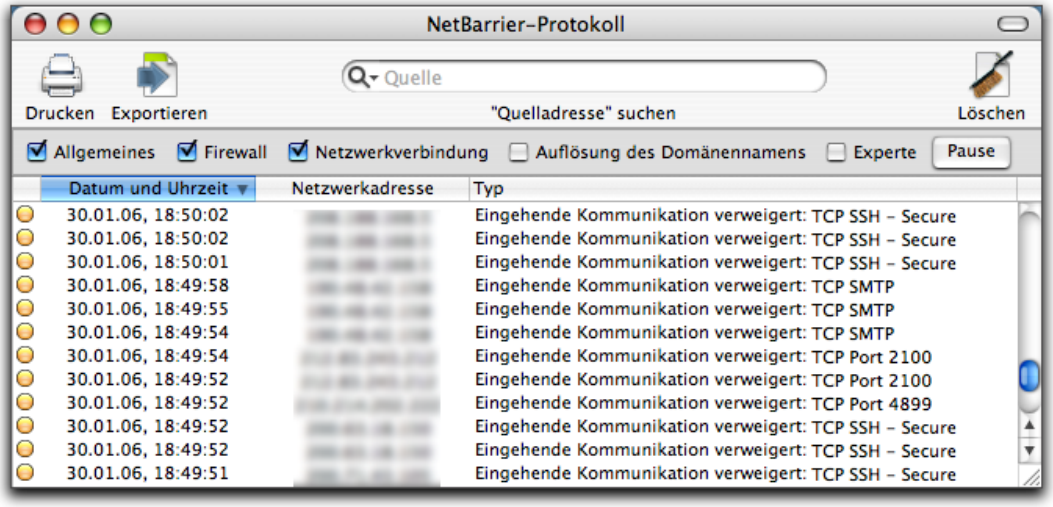
Das Protokollfenster kann auch allein angezeigt werden; das Hauptfenster von Intego NetBarrier X4 bleibt dabei unsichtbar. Wählen Sie hierzu die Menüoption „Protokollfenster öffnen“ aus dem Menü „Fenster“. Nun wird das Protokoll in einem neuen Fenster geöffnet, dessen Größe Sie verändern können, um umfangreiche Protokolle besser einsehen zu können.


NetBarrier-Protokoll
Allgemeines
Firewall
Netzwerkverbindung
Auflösung des Domänennamens
Experte
Pause
Datum und Uhrzeit
Netzwerkadresse
Typ
30.01.06, 18:31:13 Beenden von FrontEnd
30.01.06, 18:31:13 Starten von FrontEnd
30.01.06, 18:31:27 Verbindung mit: TCP POP3
30.01.06, 18:31:28 Verbindung mit: TCP POP3
30.01.06, 18:31:34 Verbindung mit: TCP POP3
30.01.06, 18:31:41 Verbindung mit: TCP POP3
30.01.06, 18:31:59 Verbindung mit: TCP HTTP – web service
30.01.06, 18:32:04 Verbindung mit: TCP SMB/CIFS – Windows file service
30.01.06, 18:32:04 Verbindung mit: TCP SMB/CIFS – Windows file service
30.01.06, 18:32:06 Verbindung mit: TCP HTTP – web service
30.01.06, 18:32:13 Verbindung mit: TCP HTTP – web service
30.01.06, 18:32:20 Verbindung mit: TCP HTTP – web service

Vorausgesetzt das Hauptfenster von NetBarrier X4 wurde gestartet, können Sie sich das Protokollfenster auch jederzeit anzeigen lassen, indem Sie die Tastenkombination „Befehl+Auswahl+L“ drücken.

Verwenden der Symbolleiste im Protokollfenster

Im Protokollfenster finden Sie eine Symbolleiste. Durch Klicken auf diese Symbole können Sie Protokolldaten filtern, ausdrucken und exportieren, und das gesamte Protokoll löschen. Ob die Symbolleiste angezeigt werden soll, können Sie mit Hilfe der Option „Ansicht“ > „Werkzeugleiste anzeigen“ wählen.


NetBarrier-Protokoll
Drucken
Exportieren
Quelle
"Quelladresse" suchen
Löschen
Allgemeines
Firewall
Netzwerkverbindung
Auflösung des Domänennamens
Experte
Pause
Datum und Uhrzeit
Netzwerkadresse
Typ
30.01.06, 18:50:02 Eingehende Kommunikation verweigert: TCP SSH – Secure
30.01.06, 18:50:02 Eingehende Kommunikation verweigert: TCP SSH – Secure
30.01.06, 18:50:01 Eingehende Kommunikation verweigert: TCP SSH – Secure
30.01.06, 18:49:58 Eingehende Kommunikation verweigert: TCP SMTP
30.01.06, 18:49:55 Eingehende Kommunikation verweigert: TCP SMTP
30.01.06, 18:49:54 Eingehende Kommunikation verweigert: TCP SMTP
30.01.06, 18:49:54 Eingehende Kommunikation verweigert: TCP Port 2100
30.01.06, 18:49:52 Eingehende Kommunikation verweigert: TCP Port 2100
30.01.06, 18:49:52 Eingehende Kommunikation verweigert: TCP Port 4899
30.01.06, 18:49:52 Eingehende Kommunikation verweigert: TCP SSH – Secure
30.01.06, 18:49:52 Eingehende Kommunikation verweigert: TCP SSH – Secure
30.01.06, 18:49:51 Eingehende Kommunikation verweigert: TCP SSH – Secure

Ob die Symbolleiste verborgen werden soll, können Sie mit Hilfe der Option „Ansicht“ > „Werkzeugleiste verbergen“ festlegen.

Ausdrucken des Protokolls

Wenn Sie das gesamte Protokoll ausdrucken wollen, müssen Sie nur auf die Schaltfläche „Drucken“ in der Symbolleiste des Protokollfensters klicken. Nun wird ein standardmäßiges Dialogfeld zum Drucken geöffnet. Aus diesem können Sie die Druckoptionen entsprechend Ihrem Drucker wählen.

Exportieren des Protokolls

Sie können das gesamte Protokoll exportieren, indem Sie auf die Schaltfläche „Exportieren…“ in der Symbolleiste des Fensters „Protokoll“ klicken. Sie können das Protokoll in sechs Formaten exportieren. Weitere Informationen hierzu finden Sie im Kapitel 6, **Exportieren des Protokolls**.)

Löschen des Protokolls

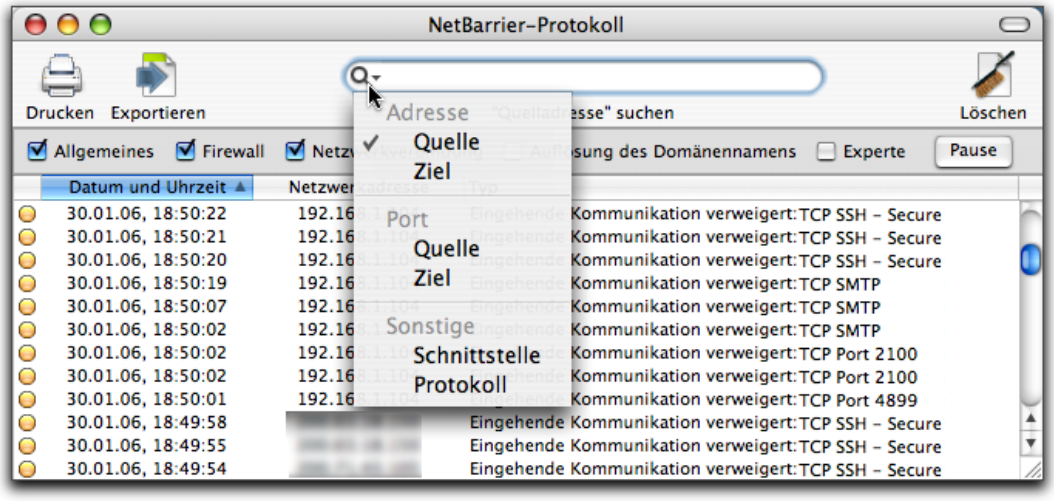
Um alle Informationen im Protokoll zu löschen, müssen Sie nur auf die Schaltfläche „Löschen…“ in der Symbolleiste des Fensters „Protokoll“ klicken. Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie das Protokoll wirklich löschen wollen. Klicken Sie auf die Schaltfläche „Löschen…“, um das Protokoll zu löschen, oder auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Filtern von Daten im Protokollfenster

Die Symbolleiste im Protokollfenster enthält ein Suchfeld zum Filtern von Daten im Protokollfenster nach bestimmten Kriterien, sodass nur noch die gewünschten Einträge angezeigt werden. Die Protokolleinträge können nach folgenden Kriterien gefiltert werden:

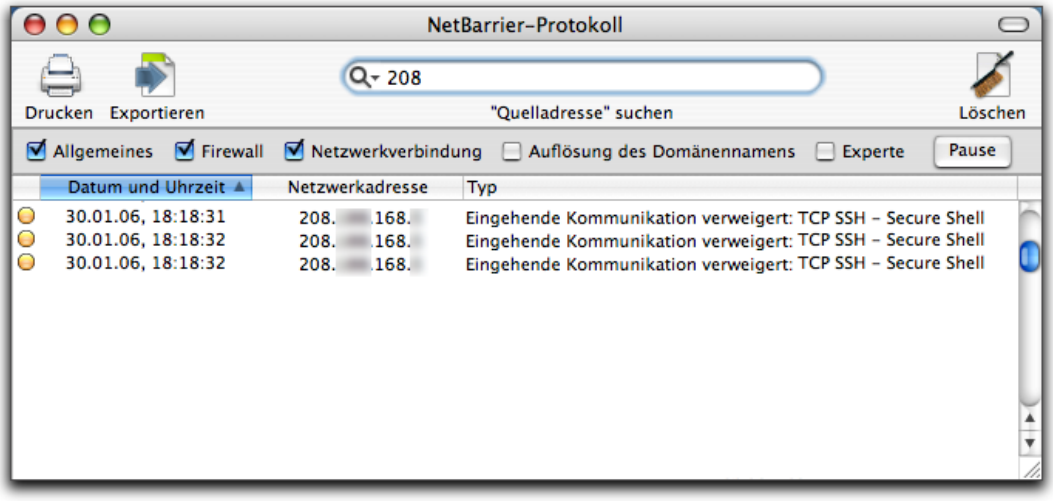
- **Quelladresse**
- **Zieladresse**
- **Quell-Port**
- **Ziel-Port**
- **Schnittstelle**
- **Protokoll**

Wenn Sie nach Protokolleinträgen suchen wollen, von denen dieser Kriterien erfüllt werden, müssen Sie aufs Schließdreieck neben der Schaltfläche „Suchen“ klicken.



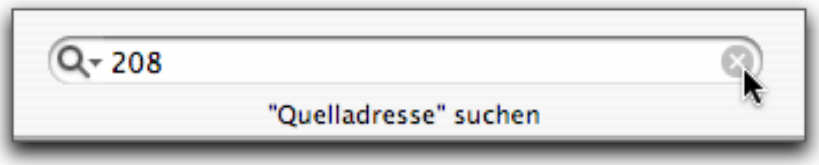
Wählen Sie das gewünschte Suchkriterium und geben Sie die Suchzeichenfolge ins Feld für die Eingabe des Suchbegriffs ein. Sie müssen nicht den gesamten Suchbegriff eingeben. Mit der Eingabe jedes weiteren Zeichens des Suchbegriffs wird die Anzahl der angezeigten Protokolleinträge entsprechend verringert.

Im nachstehenden Beispiel werden die Protokolleinträge so sortiert, dass nur Einträge mit der Ziffernfolge 208 in der Zieladresse angezeigt werden.



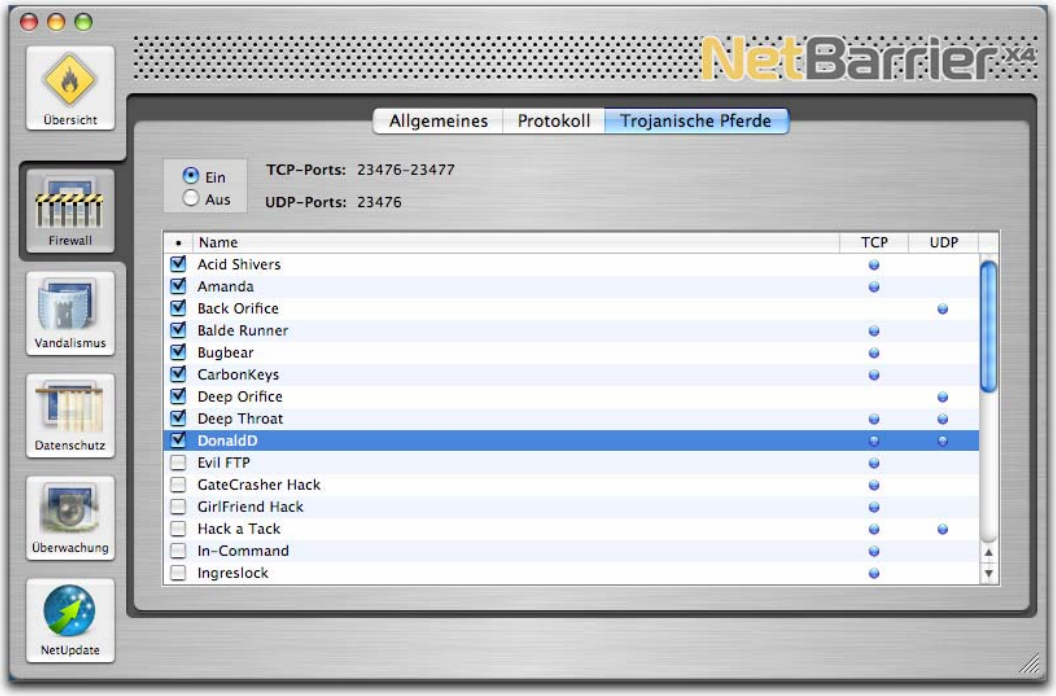
Diese dynamische Filterung funktioniert nur bei den ersten Zeichen einer Zeichenfolge. Gäben Sie die Zeichenfolge 168 ein, würde die im obigen Beispiel dargestellte Anzeige nicht erscheinen.

Wenn Sie den Inhalt des Suchfelds löschen wollen, um eine neue Suche zu starten, müssen Sie auf die Schaltfläche „Löschen“ im Suchfeld klicken.



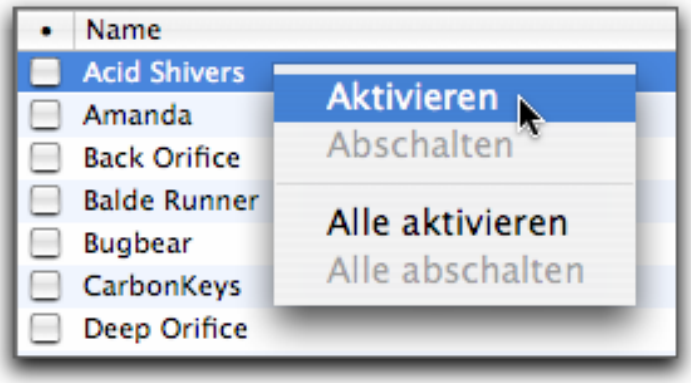
Schutz vor Trojanischen Pferden

Trojanische Pferde sind Programme, die heimlich auf Ihrem Computer installiert werden. Sie können in Anhängen von E-Mail-Mitteilungen oder in Programmen enthalten sein, die hauptsächlich Shareware (nur bei Gefallen zu bezahlende Software) oder Freeware (kostenlose Software) sind. In manchen Fällen installieren Programme eine bestimmte Art von Trojanischem Pferd. Diese als Spyware bezeichnete Software sendet persönliche Informationen an einen Server. Da die Verbindung von *Ihrem* Computer aus hergestellt wird, ist dies normalerweise nicht auffällig. Intego NetBarrier X4 ist jedoch in der Lage, die Aktivitäten der meisten Trojanischen Pferde zu erkennen und diese zu blockieren. Bei den heimlich von Trojanischen Pferden gesendeten Informationen kann es sich um Informationen über das Surfverhalten des Benutzers handeln. Andere Trojanische Pferde öffnen *Hintertüren* in Ihrem Computer, um einen Außenstehenden die Kontrolle über Ihren Computer übernehmen zu lassen, sodass dieser beispielsweise auch Dateien auf Ihrer Festplatte löschen kann.



Sie können den Schutz vor Trojanischen Pferden durch Klicken auf die Schaltfläche „Ein“ aktivieren. Nun müssen Sie noch auf die Kontrollkästchen für die Trojanischen Pferde klicken, vor denen Ihr Computer geschützt sein soll.

Sie können den Schutz vor Trojanischen Pferden auch nur für ein einzelnes Trojanisches Pferd oder für alle Trojanischen Pferde aktivieren. Klicken Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh auf den Namen des betreffenden Trojanischen Pferds. Nun wird ein Kontextmenü geöffnet.



Wählen Sie die Menüoption „Aktivieren“ fürs gewünschte Trojanische Pferd oder die Menüoption „Alle aktivieren“, um den Schutz für alle Trojanischen Pferde zu aktivieren.

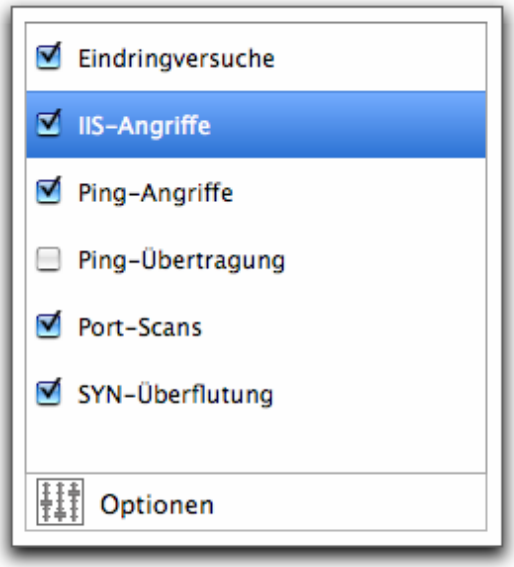
Auf die gleiche Weise können Sie den Schutz vor einzelnen oder allen Trojanischen Pferden abschalten.

Antivandalismus

Dank seiner integrierten Funktion „Antivandalismus“ ist Intego NetBarrier X4 in der Lage, alle bei Ihrem Computer eingehenden Datenpakete daraufhin zu überwachen, ob jemand versucht, in Ihren Computer einzudringen. Bei Bedarf werden diese eingehenden Datenpakete gefiltert. Die Filterung erfolgt transparent. Intego NetBarrier X4 tritt nur dann in Erscheinung, nachdem verdächtige Datenpakete entdeckt wurden. In diesem Fall wird ein Fenster mit einer Warnmeldung geöffnet. Andernfalls überwacht die Funktion „Antivandalismus“ von Intego NetBarrier X4 kontinuierlich alle Netzwerkaktivitäten Ihres Computers im Hintergrund.

Richtlinie

Auf der Registerkarte „Richtlinie“ werden mehrere Optionen für die Richtlinien zur Auswahl angeboten, mit denen der Schutz von Intego NetBarrier X4 vor dem Eindringen in Ihren Computer konfiguriert werden kann.



IIS-Angriffe

Wenn dieses Kontrollkästchen markiert ist, erkennt Intego NetBarrier X4 CodeRed- und Nimda-Anfragen, die an Ihren Computer gesendet werden, wenn dieser als Website-Server arbeitet oder wenn Sie einen Server haben, der Anfragen an HTTP-Ports empfängt. Hierdurch wird Ihr Computer vor DoS-Angriffen geschützt.

Eindringversuche

Wenn dieses Kontrollkästchen markiert ist, sendet Ihnen Intego NetBarrier X4 eine E-Mail-Mitteilung, nachdem dreimal nacheinander versucht wurde, sich mit einem falschen Passwort bei Ihrem Computer anzumelden. Dies gilt

beispielsweise für Verbindungsversuche in Verbindung mit Webfreigabe, Datei- und Druckerfreigabe oder FTP.

Ping-Angriffe

Wenn dieses Kontrollkästchen markiert ist, werden Ping-Angriffe automatisch gesperrt. Ping-Datentelegramme werden akzeptiert, doch wenn die Anzahl oder Häufigkeit der Ping-Anfragen die voreingestellten Grenzwerte überschreitet, werden sie gesperrt.

Ping-Übertragung

Wenn dieses Kontrollkästchen markiert ist, werden Ping-Übertragungen automatisch gesperrt.

Schutz vor „Port Scans“

Wenn dieses Kontrollkästchen markiert ist, wird das Suchen nach offenen Ports auf Ihrem Computer automatisch gesperrt. Wenn Sie Ihren Computer als Server einsetzen, ist es unter Umständen besser, dieses Kontrollkästchen nicht zu markieren.

SYN-Überflutung

Wenn dieses Kontrollkästchen markiert ist, wird die Anzahl eingehender Verbindungen auf Ihrem Computer automatisch begrenzt, um DoS-Angriffen vorzubeugen.

Optionen

Im Bereich „Optionen“ der Registerkarte „Richtlinien“ stehen zusätzliche Filteroptionen zur Verfügung.

Tarnkappenmodus (verhindert Antworten auf Pings)

Wenn dieses Kontrollkästchen markiert ist, bleibt Ihr Computer für andere Computer im Internet oder in einem lokalen Netzwerk unsichtbar. Allerdings bleiben Sie nicht anonym: alle von Ihren Computer gesendeten Anfragen werden mit der IP-Nummer Ihres Computers identifiziert.

Sperren unbekannter Protokolle

Wenn dieses Kontrollkästchen markiert ist, werden alle unbekannten Protokolle automatisch gesperrt.

Keine Fernsteuerung mit ARD Control zulassen

Wenn dieses Kontrollkästchen markiert ist, sperrt NetBarrier X4 alle Aktivitäten von Apple Remote Desktop.

Ermöglichen von FTP-Dateitransfers im PORT-Modus

Wenn dieses Kontrollkästchen markiert ist, können Sie FTP-Dateitransfers durchführen, wenn Ihr Computer im Firewall-Modus „Nur Client“ arbeitet.

E-Mail

Wenn Sie Benachrichtigungen über Alarmmeldungen per E-Mail erhalten möchten, müssen Sie Ihre E-Mail-Einstellungen konfigurieren. Klicken Sie auf die Schaltfläche „Konfigurieren…“ und geben Sie die richtigen Informationen für Ihre Mail-Einstellungen ein. In die drei Felder müssen Sie den Namen des Absenders, die E-Mail-Adresse des Empfängers und den Namen des SMTP-Servers (für ausgehende E-Mail-Mitteilungen) eingegeben werden. E-Mail-Nachrichten können an mehrere Empfänger versendet werden. Klicken Sie auf die Schaltfläche „+“, um einen Empfänger hinzuzufügen. Klicken Sie auf die Schaltfläche „-“, um einen Empfänger zu löschen.

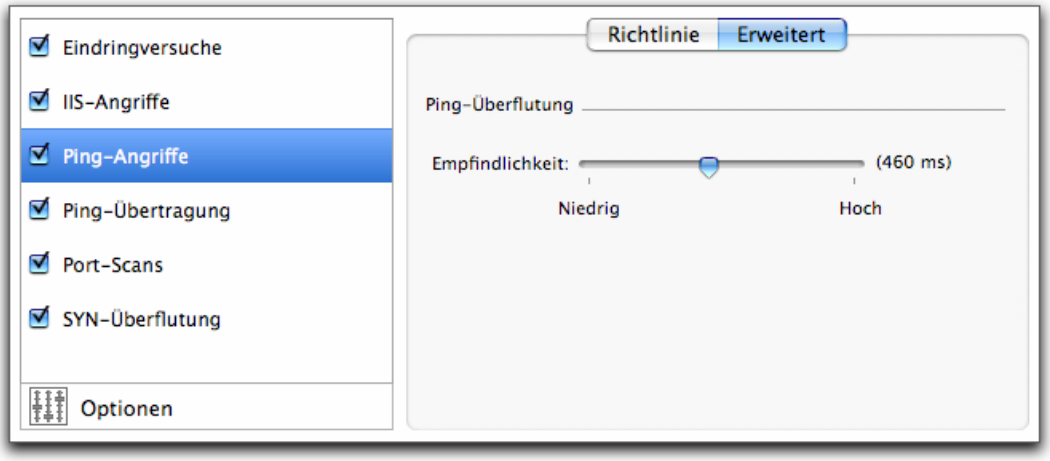
Wenn Ihr Mailserver eine Authentifizierung für das Versenden von E-Mail-Nachrichten erfordert, sollten Sie die untere Hälfte des Fensterabschnitts ausfüllen. Wenden Sie sich an Ihren Systemadministrator, wenn Sie nicht genau wissen, ob Ihr Mailserver eine Authentifizierung erfordert.

Richtlinie

Wenn Sie für alle verschiedenen Arten des Schutzes, die NetBarrier X4 bietet, die gleichen Richtlinieneinstellungen verwenden möchten, markieren Sie einfach das Kästchen neben der Option „Für alle Schutzarten die gleiche Richtlinie verwenden“. Entfernen Sie das Häkchen aus diesem Kästchen, wenn Sie individualisierte, benutzerdefinierte Richtlinieneinstellungen für jede Schutzart verwenden möchten.

Einstellen der Empfindlichkeit gegenüber Ping-Überflutung

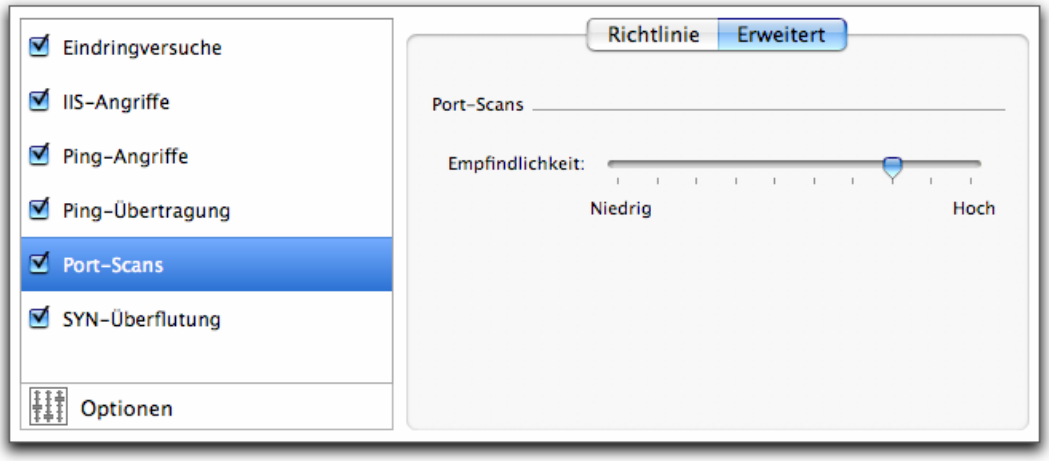
Sie können die Empfindlichkeit von Intego NetBarrier X4 gegenüber Ping-Angriffen einstellen. Wenn Ihr Computer in ein Netzwerk integriert ist, ist es vollkommen normal, was der Netzwerkverwalter Ihren Computer gelegentlich per Ping „anbimmelt“. Wenn Ihr Computer nicht in ein Netzwerk integriert ist, gibt es allerdings keinerlei Grund, an ihn Ping-Anfragen zu senden. Die einzige Ausnahme hiervon dürfte der Fall sein, wenn Sie Ihren Computer über ein DSL- oder Kabelmodem mit dem Internet verbunden haben und Ihr ISP Ihrem Computer ab und zu eine Ping-Anfrage sendet, um zu prüfen, ob Ihr Computer mit dem Kabelnetzwerk verbunden ist.



Wenn Sie die Empfindlichkeit gegenüber Ping-Überflutung anpassen möchten, wählen Sie „Ping-Angriffe“ und klicken Sie auf die Registerkarte „Erweitert“. Schieben Sie die blaue Markierung nach links, um die Empfindlichkeit zu verringern oder nach rechts, um die Empfindlichkeit zu erhöhen. Wenn Ihr Computer mit einem Netzwerk verbunden ist und Sie zu viele Warnmeldungen erhalten, sollten Sie die Empfindlichkeit gegenüber Ping-Überflutung reduzieren.

Einstellen der Empfindlichkeit gegenüber Port-Scans

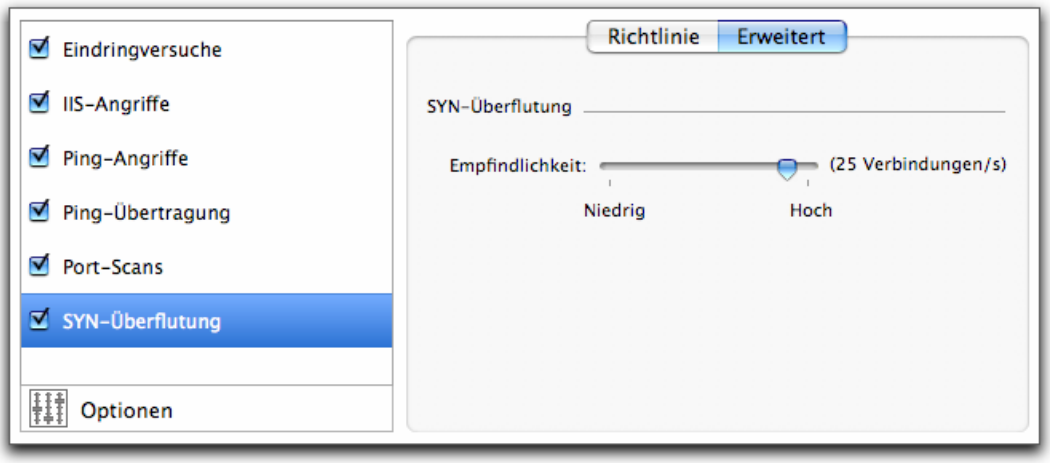
Sie können die Empfindlichkeit von NetBarrier X4 gegenüber Port-Scans (Abfragen Ihres Computers auf offene Ports, um ihn eventuell attackieren zu können) einstellen.



Wenn Sie die Empfindlichkeit gegenüber Port-Scans anpassen möchten, wählen Sie „Port-Scans“ und klicken Sie auf die Registerkarte „Erweitert“. Schieben Sie die blaue Markierung nach links, um die Empfindlichkeit zu verringern oder nach rechts, um die Empfindlichkeit zu erhöhen. Wenn Ihr Computer mit einem Netzwerk verbunden ist und Sie zu viele Warnmeldungen erhalten, sollten Sie die Empfindlichkeit gegenüber Port-Scans reduzieren.

Einstellen der Empfindlichkeit gegenüber SYN-Überflutung

Sie können die Empfindlichkeit von Intego NetBarrier X4 gegenüber SYN-Überflutung einstellen.



Wenn Sie die Empfindlichkeit gegenüber SYN-Überflutung anpassen möchten, wählen Sie „SYN-Überflutung“ und klicken Sie auf die Registerkarte „Erweitert“. Schieben Sie die blaue Markierung nach links, um die Empfindlichkeit zu verringern oder nach rechts, um die Empfindlichkeit zu erhöhen. Wenn Ihr Computer mit einem Netzwerk verbunden ist und Sie zu viele Warnmeldungen erhalten, sollten Sie die Empfindlichkeit gegenüber SYN-Überflutung reduzieren.

Warnmeldungen

Die Bedeutung von Warnmeldungen

Intego NetBarrier X4 überwacht kontinuierlich die Netzwerkaktivitäten Ihres Computers, u.z. unabhängig davon, ob dieser mit einem lokalen Netzwerk oder dem Internet verbunden ist. Intego NetBarrier X4 ist so vorkonfiguriert, dass nach Datenpaketen gesucht wird, die auf einen Eindringversuch oder einen Angriff hinweisen. Wenn verdächtige Datenpakete gefunden werden, gibt Intego NetBarrier X4 eine Warnmeldung aus, wobei Sie gleichzeitig gefragt werden, ob das Senden der Datenpakete zugelassen oder verweigert werden soll.

Nachstehend sehen Sie ein typisches Beispiel für eine Warnmeldung. In der oberen Zeile sehen Sie den Grund der Warnmeldung. In diesem Fall handelt es sich um einen Eindringversuch. Ein Server mit der IP-Adresse 10.0.1.90 versuchte, Ihren Computer mit Ping-Überflutung anzugreifen. Durch Klicken auf eine der beiden Schaltflächen auf der unteren rechten Seite können Sie festlegen, was nun geschehen soll.

Wenn Sie auf die HyperText-Verknüpfung „Weitere Informationen…“ unten links klicken, wird ein Fenster mit Informationen über die Ursache der Warnmeldung Informationsfenster geöffnet.

Wenn Sie auf die Schaltfläche zum Überprüfen der DNS klicken (das ?), können Sie zwischen der numerischen IP-Adresse und dem aktuellen Domänennamen des Angreifers hin- und herschalten, sofern es einen gibt.

Auf Alarme können Sie wie folgt reagieren:

Sperrliste

In den meisten Fällen sollten Sie auf eine Warnmeldung von Intego NetBarrier X4 durch Klicken auf die Schaltfläche „Sperrliste“ reagieren. Wenn Sie auf diese Schaltfläche klicken oder die Eingabetaste in der Tastatureinheit Ihres Computers drücken, wird der Empfang der Datenpakete von diesem Server gesperrt, sodass der Eindringversuch abgewehrt wird. Das empfangene Datenpaket wird nun ignoriert, als wäre es niemals empfangen worden. Wenn das empfangene Datenpaket Bestandteil einer Datei ist, so wird diese ebenfalls von Ihrem Computer ignoriert. Wenn das empfangene Datenpaket ein Befehl ist, wird er ebenfalls ignoriert und nicht ausgeführt.

Wenn Sie auf die Schaltfläche „Sperrliste“ klicken, wird die IP-Nummer des Computers, der das Datenpaket an Ihren Computer gesandt hatte, automatisch in die Sperrliste aufgenommen und in dieser über die standardmäßig definierte Zeitdauer gespeichert. (Weitere Informationen hierzu finden Sie im Unterabschnitt **Sperrliste** des Kapitels 5.) Diese Zeitdauer kann im Popup-Menü geändert werden.

Ignorieren

Wenn Sie auf diese Schaltfläche klicken, werden die Daten von Ihrem Computer empfangen. Der Datentransfer wird wie gewöhnlich fortgesetzt, bis Intego NetBarrier X4 einen weiteren Eindringversuch erkennt. In diesem Fall wird ein anderes Fenster mit einer Warnmeldung geöffnet.

Angriffszähler

Intego NetBarrier X4 protokolliert die Anzahl der Angriffe, vor denen Ihr Computer geschützt wurde, und zeigt diese Anzahl in einem Zähler am unteren Rand des Fensters „Richtlinien“ auf der Registerkarte „Vandalismus“ an. Hier wird auch angezeigt, welche Art von Angriff zuletzt abgewehrt wurde, und wann dieser Angriff stattfand.

Sie können den Angriffszähler durch Klicken auf die daneben befindliche Schaltfläche „Zurücksetzen“ auf Null zurücksetzen.

Warnmeldungen

Intego NetBarrier X4 kann Sie warnen, wenn ein Angriff stattfindet. Für jede Angriffsart können verschiedene Optionen dafür festgelegt werden, wie Intego NetBarrier X4 reagieren soll, wenn eine Warnung ausgegeben wurde. So können Sie jeweils die Konfiguration auswählen, die Ihren Bedürfnissen entspricht.

Eingeben in die Sperrliste für:

Wenn dieses runde Optionsfeld markiert ist, werden die Verbindungen bei der Ausgabe einer Warnmeldung automatisch unterbrochen. Die IP-Adresse des angreifenden Computers wird automatisch in die Sperrliste aufgenommen. (Weitere Informationen hierzu finden Sie im Unterabschnitt **Sperrliste** des Kapitels 5.) In einem Feld rechts vom runden Optionsfeld können Sie angeben, wie lang die IP-Adresse in der Sperrliste gespeichert werden soll. Sie können diese Zeitdauer in Sekunden, Minuten, Stunden oder Tagen angeben oder

festlegen, dass die IP-Adresse des angreifenden Computers auf Dauer in der Sperrliste gespeichert werden soll.

Fragen

Wenn dieses runde Optionsfeld markiert ist, öffnet Intego NetBarrier X4 bei jedem erkannten Eindringversuch ein Fenster mit einer Warnmeldung, wobei Sie gefragt werden, anzugeben, was nun geschehen soll. In diesem Fenster mit der Warnmeldung wird auch die Zeitdauer angezeigt, worüber die IP-Nummer des angreifenden Computers standardmäßig in der Sperrliste gespeichert wird. Diese Zeitdauer können Sie auf der Registerkarte „Warnmeldungen“ ändern.

Dialogfeld in den Vordergrund bringen

Wenn dieses Kontrollkästchen markiert ist, werden Fenster mit einer Warnmeldung von Intego NetBarrier X4 automatisch in den Vordergrund gebracht. Andernfalls bleiben diese Fenster im Hintergrund (also hinter eventuellen anderen Fenstern auf dem Bildschirm Ihres Computers). Wenn Sie 90 Sekunden lang nicht auf eine Warnmeldung reagieren, wird das Fenster automatisch geschlossen. Die betreffende Verbindung mit Ihrem Computer wird verweigert.

Text der Warnmeldung vorlesen

Wenn dieses Kontrollkästchen markiert ist, wird der Text der Warnmeldung mit Hilfe der in Mac OS X implementierten Funktion „Text-to-Speech“ vorgelesen.

Nicht fragen, wenn der momentane Benutzer kein Systemverwalter ist

Wenn dieses Kontrollkästchen markiert ist, fragt Intego NetBarrier X4 nicht nach, ob der aktuelle Benutzer Systemverwalter ist, und trägt die Internet-Adresse des anderen Computers automatisch in die Sperrliste ein.

Sound abspielen

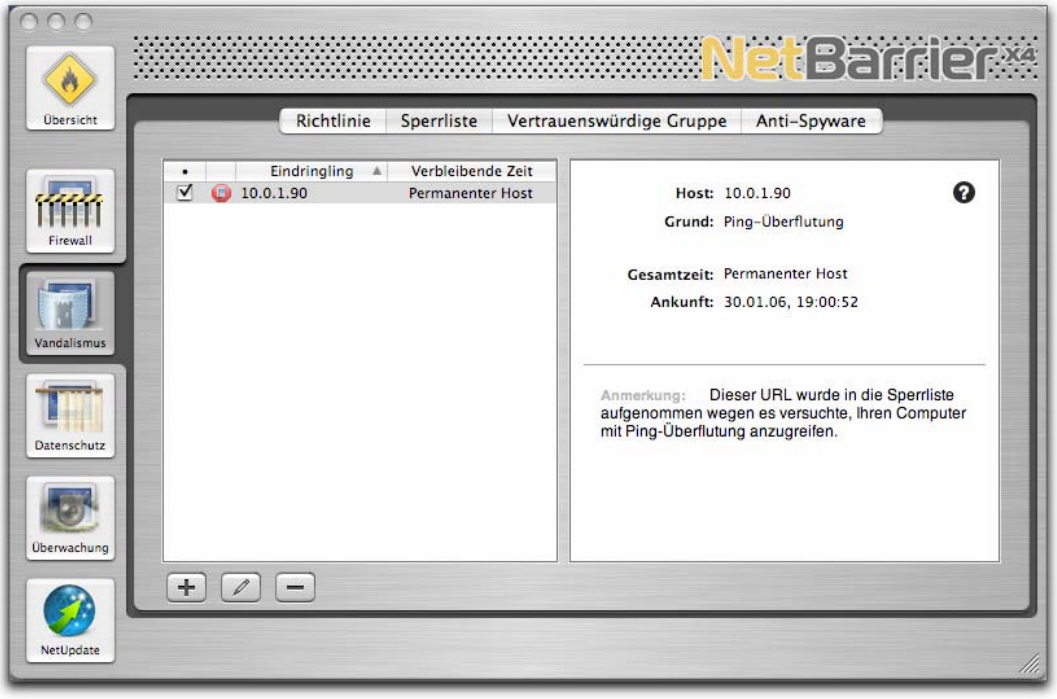
Wenn dieses Kontrollkästchen markiert ist, ertönt bei jedem entsprechenden Ereignis ein akustischer Alarm. Aus dem Popup-Menü rechts vom Kontrollkästchen „Sound abspielen“ können Sie die gewünschte Klangdatei wählen.

E-Mail-Mitteilung senden

Wenn dieses Kontrollkästchen markiert ist, sendet Intego NetBarrier X4 innerhalb von 30 Sekunden automatisch eine E-Mail-Mitteilung an die Adresse, die auf der Registerkarte „Optionen“ (siehe oben) konfiguriert wurde. (Intego NetBarrier X4 wartet, ob noch andere Eindringversuche stattfinden, bevor die E-Mail-Mitteilung gesendet wird.)

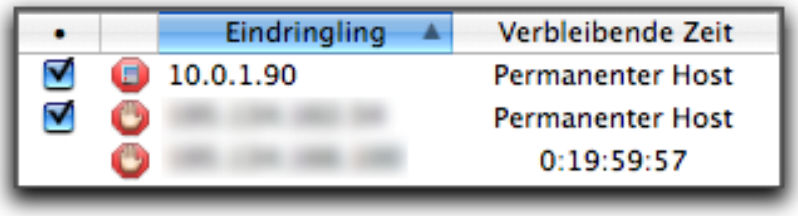
Die Sperrliste

Die Sperrliste ist eine leistungsstarke Funktion von Intego NetBarrier X4. Damit können Sie den Empfang von Datenpaketen von Computern mit in die Sperrliste aufgenommenen Internet-Adressen sperren. Auch Ihr Computer kann keine Verbindung mit einem Computer herstellen, dessen Internet-Adresse in der Sperrliste gespeichert ist. Die Internet-Adresse eines angreifenden Computers kann über eine von Ihnen definierbare Zeitdauer oder aber permanent in der Sperrliste gespeichert werden. Die standardmäßige Zeitdauer können Sie auf der Registerkarte „Richtlinie“ ändern (siehe oben).



In der Sperrliste angezeigte Informationen

Auf der Registerkarte „Sperrliste“ werden die IP-Adressen von Computern angezeigt, die derzeit in der Sperrliste gespeichert sind.



Eindringling

Die IP-Nummer des angreifenden Computers.

Verbleibende Zeit

Die Zeitdauer (Verweildauer), worüber die IP-Nummer des angreifenden Computers in der Sperrliste gespeichert wird.

Wenn die IP-Adresse des anderen Computers auf Dauer in die Sperrliste eingetragen ist, erscheint links davon ein Kontrollkästchen. Wenn der andere Computer in der Lage sein soll, vorübergehend eine Verbindung mit Ihrem Computer herzustellen, können Sie die Markierung aus dem Kontrollkästchen entfernen. Sie müssen ihn als nicht aus der Sperrliste löschen. Wenn Sie den anderen Computer wieder sperren wollen, müssen Sie nur das Kontrollkästchen links von seiner Internet-Adresse markieren.

Andere in der Sperrliste angezeigte Informationen

Wenn Sie einmal auf eine Internet-Adresse in der Sperrliste klicken, werden in der rechten Hälfte der Registerkarte „Sperrliste“ weitere Informationen angezeigt.

Host: 10.0.1.90
Grund: Ping-Überflutung
Gesamtzeit: 20:00:00:00
Ankunft: 31.01.06, 10:05:22
Start: 20.02.06, 10:05:22
Anmerkung: Dieser URL wurde in die Sperrliste aufgenommen wegen es versuchte, Ihren Computer mit Ping-Überflutung anzugreifen.

Host

An der Oberseite dieses Bereichs wird die IP-Nummer des angreifenden Computers angezeigt. Wenn Sie auf die Schaltfläche zum Überprüfen der DNS klicken (das ?), können Sie zwischen der numerischen IP-Adresse und dem aktuellen Domänennamen des Angreifers hin- und herschalten, sofern es einen gibt. Sie können sich diese Adresse in großer Schrift anzeigen lassen. Verschieben Sie hierzu den Mauszeiger über das Etikett „Host“, bis es hervorgehoben dargestellt wird, klicken Sie mit der Maus darauf und wählen Sie aus dem Kontextmenü die Option „Große Schrift“.

Grund

In einer Textzeile wird mitgeteilt, aus welchem Grund die IP-Adresse in die Sperrliste aufgenommen wurde (in diesem Beispiel geschah das wegen eines Angriffs mit Ping-Überflutung).

Gesamtzeit

Die **Gesamtzeit** ist der Zeitraum, über den die IP-Adresse des anderen Computers in der Sperrliste verbleibt. Wenn Sie auf „Gesamtzeit“ klicken, können Sie sich den verbleibenden Zeitraum anzeigen lassen, über den die Adresse des Angreifers noch in der Sperrliste gespeichert wird. Wenn Sie auf „Verbleibende Zeit“ klicken, wird Ihnen der bisher abgelaufene Zeitraum angezeigt. So erfahren Sie, wie lange die Adresse des Angreifers bereits in der Sperrliste gespeichert ist. Wenn Sie auf „Abgelaufene Zeit“ klicken, wird Ihnen noch einmal die Gesamtzeit angezeigt.

Ankunft

Im Abschnitt „Ankunft“ erfahren Sie, wann die Adresse der Sperrliste hinzugefügt wurde.

Start

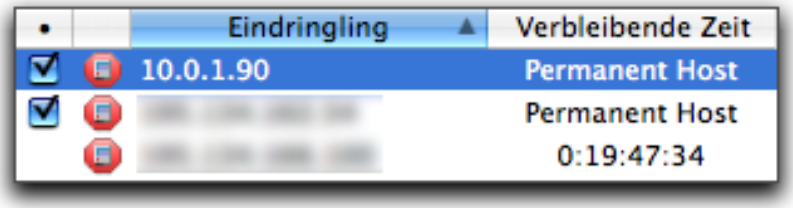
Im Abschnitt „Start“ erfahren Sie, wann die Adresse von der Sperrliste gestrichen wird. Sie können diesen Zeitpunkt ändern, indem Sie den Mauszeiger über das Etikett „Start“ ziehen, bis es hervorgehoben wird. Dann klicken Sie darauf, wählen die Menüoption „Hinzufügen“ oder „Entfernen“ und wählen anschließend den Zeitraum aus, um den Sie die Gesamtzeit verlängern oder verkürzen wollen.

ANMERKUNG:

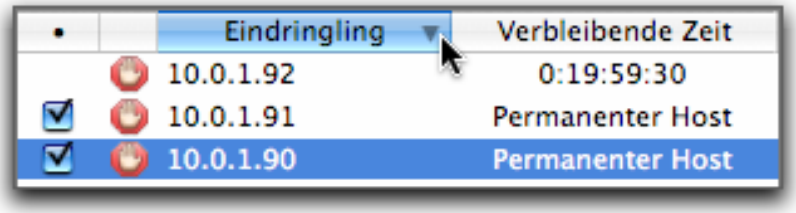
Im Textfeld in der unteren Hälfte dieses Abschnitts werden Anmerkungen angezeigt, die Sie zur betreffenden IP-Adresse in die Sperrliste eingegeben haben oder die von Intego NetBarrier X4 generiert wurden. Weitere Informationen über das Eingeben oder Hinzufügen von Anmerkungen zu einem Sperrlisteneintrag finden Sie weiter unten.

Ändern der Listenanzeige

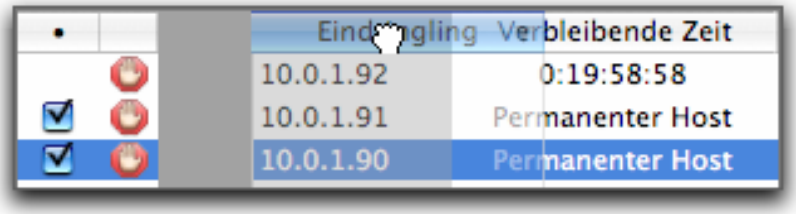
Sie können den Inhalt der Sperrliste nach Spalteninhalten sortieren, indem Sie auf die Spaltenüberschrift klicken.



Durch Klicken aufs Sortierdreieck rechts neben der aktivierten Spaltenüberschrift können Sie die Sortierreihenfolge von auf- in absteigend ändern.



Sie können auch die Reihenfolge der Spalten ändern. Klicken Sie hierzu in die Überschrift der gewünschten Spalte, halten Sie die Maustaste gedrückt und ziehen Sie die Überschrift in die gewünschte Position. Lassen Sie die Maustaste wieder los.



Hinzufügen von Internet-Adressen zur Sperrliste

Internet-Adressen können auf drei unterschiedliche Arten in die Sperrliste aufgenommen werden. Das erste Verfahren ist die Reaktion auf die Ausgabe einer Warnmeldung. (Weitere Informationen hierzu finden Sie im Unterabschnitt **Warnmeldungen** weiter oben.) Wenn ein Fenster mit einer Warnmeldung geöffnet wird und Sie auf die Schaltfläche „Sperrliste“ klicken, wird die IP-Adresse des angreifenden Computers automatisch in die Sperrliste aufgenommen.

Die zweite Möglichkeit besteht darin, eine IP-Nummer aus dem Protokoll zu wählen und dann im Kontextmenü die Option „Zur Sperrliste hinzufügen“ zu wählen. Weitere Informationen hierzu finden Sie im Unterabschnitt **Kontextmenü des Protokollfensters** weiter oben.

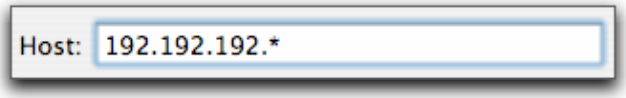
Sie können Internet-Adressen auch manuell zur Sperrliste hinzufügen. Klicken Sie hierzu auf die Schaltfläche „Hinzufügen…“. Nun wird das Dialogfeld „Sperrlisten-Editor“ geöffnet.

Geben Sie ins Feld „Host:“ die Adresse eines Computers ein. Wählen Sie, über welchen Zeitraum diese in der Sperrliste gespeichert bleiben soll, indem Sie ins Feld

„Dauer“ eine entsprechende Zahl eingeben. Die Zeiteinheit können Sie aus dem Popup-Menü wählen. Wenn Sie die numerische IP-Adresse des anderen Computers, die Sie in die Sperrliste aufnehmen wollen, nicht kennen, müssen Sie seinen Domänennamen eingeben und auf die Schaltfläche mit dem Fragezeichen (**?**) klicken. Intego NetBarrier X4 fragt nun den DNS-Server Ihres ISP (Internet Service Provider = Internet-Dienstleister) an und trägt die korrekte IP-Nummer ins Feld ein. Ins Feld „Anmerkung:“ können Sie auch Anmerkungen wie z.B. den Grund für die Aufnahme der Internet-Adresse in die Sperrliste eingeben. Wenn Sie die Internet-Adresse nicht in die Sperrliste eingeben wollen, müssen Sie nur auf die Schaltfläche „Abbrechen“ klicken.

Verwenden von Platzhalterzeichen in der Sperrliste

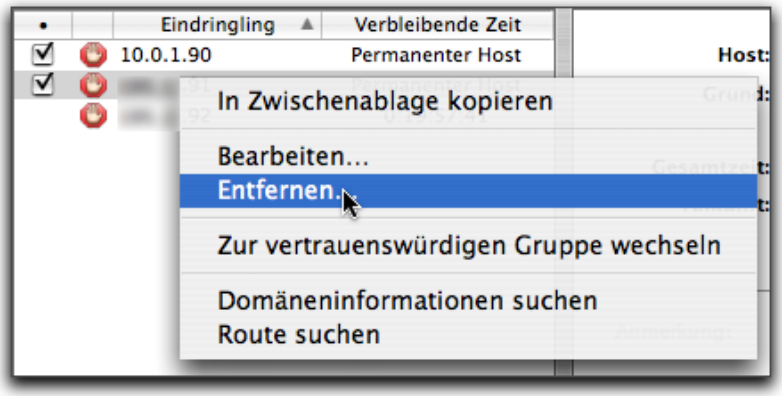
Sie können in IP-Adressen Platzhalterzeichen verwenden, um ganze Bereiche von IP-Nummern zu sperren. Geben Sie hierzu den ersten Teil einer IP-Nummer und dann eines oder mehrere Sternchen (*) ein: 192.*.*.*, 192.192.*.* oder 192.192.192.*. Hierdurch werden alle IP-Nummern gesperrt, in denen die eingegebenen Ziffern enthalten sind. Jedes Sternchen kann für eine beliebige Ziffer stehen.



Entfernen von Internet-Adressen aus der Sperrliste

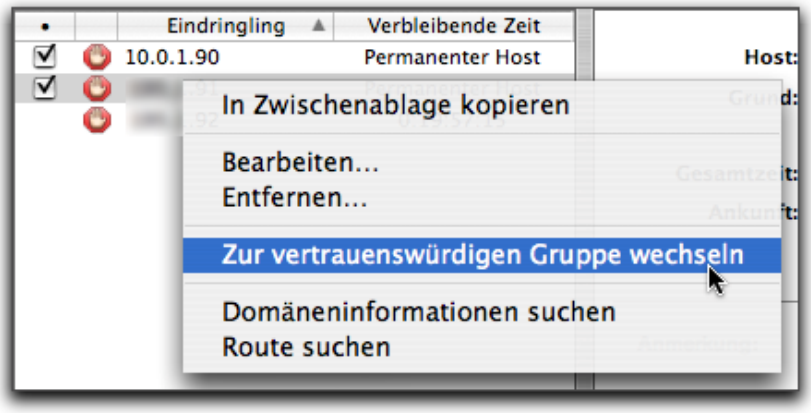
Wenn Sie eine Internet-Adresse aus der Sperrliste löschen wollen, müssen Sie einmal auf die betreffende Internet-Adresse und dann auf die Schaltfläche „Entfernen“ klicken. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie die Internet-Adresse wirklich löschen wollen. Klicken Sie dann auf die Schaltfläche „Entfernen“. Die Internet-Adresse ist nun gelöscht. Wenn Sie die Internet-Adresse nicht löschen wollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken. Sie können mehrere nacheinander in der Liste angezeigte Internet-Adressen wählen, indem Sie auf eine dieser Internet-Adressen und dann bei gedrückter Umschalttaste auf die letzte der gewünschten Internet-Adressen klicken. Bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh können Sie auch Internet-Adressen auswählen, die nicht nacheinander in der Liste angezeigt werden.

Sie können eine Internet-Adresse auch aus der Sperrliste löschen, indem Sie die Option „Entfernen…“ bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh aus dem Kontextmenü wählen. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie die Internet-Adresse wirklich löschen wollen. Klicken Sie dann auf die Schaltfläche „OK“. Die Internet-Adresse ist nun gelöscht. Wenn Sie die Internet-Adresse nicht löschen wollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.



Verschieben von Internet-Adressen aus der Sperrliste in die vertrauenswürdige Gruppe

Wenn Sie eine Internet-Adresse aus der Sperrliste in die vertrauenswürdige Gruppe verschieben wollen, müssen Sie die Menüoption „Zur vertrauenswürdigen Gruppe wechseln“ bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh aus dem Kontextmenü wählen.



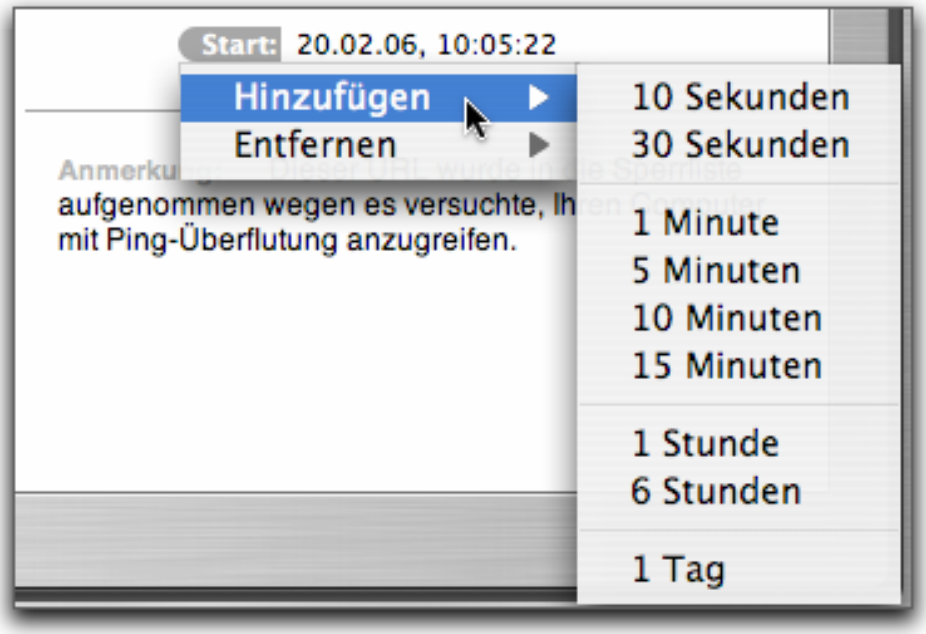
Hierdurch wird die Internet-Adresse in die vertrauenswürdige Gruppe aufgenommen. Informationen über die vertrauenswürdige Gruppe finden Sie im Unterabschnitt **Vertrauenswürdige Gruppe** weiter unten in diesem Kapitel.

Ändern einer Internet-Adresse in der Sperrliste

Wenn Sie eine Adresse in der Sperrliste bearbeiten möchten, klicken Sie erst auf die entsprechende Adresse und dann auf die Schaltfläche mit dem Bleistift auf der unteren linken Seite des Fensterabschnitts. (Sie können auch auf die Adresse doppelklicken oder bei gedrückter Steuerungstaste auf die Adresse klicken und anschließend „Bearbeiten…“ auswählen.)

Nun wird das Fenster „Sperrlisten-Editor“ geöffnet, in dem Sie die Internet-Adresse, Anmerkungen und die Verweildauer der Internet-Adresse in der Sperrliste ändern können. Um die Änderungen wirksam werden zu lassen, müssen Sie auf die Schaltfläche „OK“ klicken. Wenn die Änderungen nicht wirksam werden sollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.

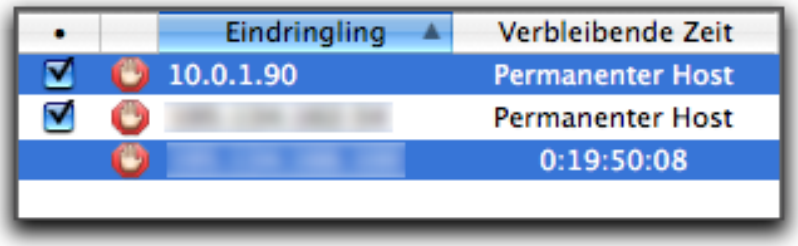
Sie können auch das Kontextmenü dazu verwenden, um die Verweildauer der Internet-Adresse in der Sperrliste zu ändern. Verschieben Sie hierzu den Mauszeiger über das Etikett „Start“ in der Sperrliste, bis es hervorgehoben dargestellt wird. Klicken Sie auf dieses Etikett und wählen Sie dann die Menüoption „Hinzufügen“ oder „Entfernen“. Wählen Sie dann einen Zeitraum aus dem Popup-Menü.



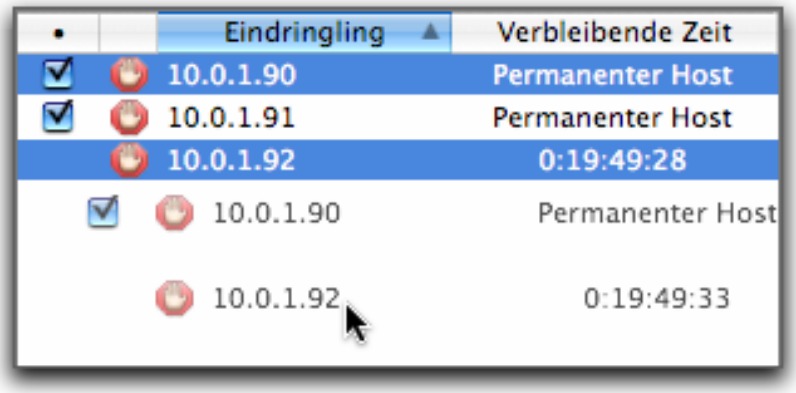
Wählen Sie die Zeit, um die Sie die Verweildauer der Internet-Adresse in der Sperrliste verlängern oder verkürzen wollen. Diese Zeit wird sofort zur bisherigen Verweildauer addiert oder von dieser subtrahiert.

Kopieren von Internet-Adressen aus der Sperrliste

Sie können Internet-Adressen aus der Sperrliste wählen und in die Zwischenablage kopieren, um sie dann in ein Dokument eines anderen Anwendungsprogramms einzusetzen. Klicken Sie hierzu auf eine Zeile in der Sperrliste und dann gleichzeitig die Befehlstaste und die Taste „C“, um die Internet-Adresse in die Zwischenablage zu kopieren. Sie können mehrere untereinander in der Sperrliste aufgeführte Internet-Adressen auswählen, indem Sie die Umschalttaste gedrückt halten. Durch Gedrückthalten der Befehlstaste können Sie auch mehrere nicht untereinander aufgeführte Internet-Adressen kopieren.

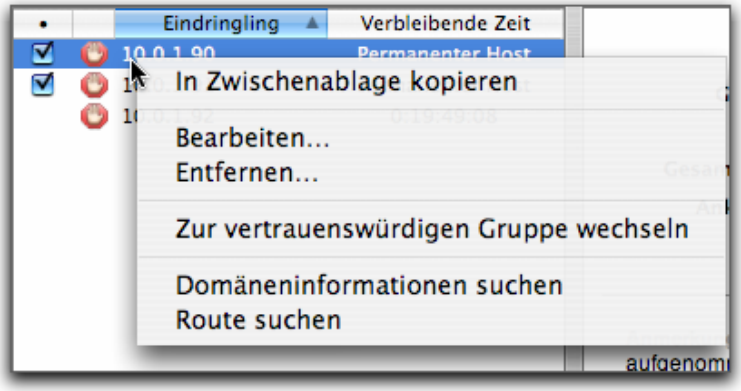


Sie können gewählte Internet-Adressen ins Fenster eines anderen Anwendungsprogramms ziehen und dort ablegen. Wählen Sie wie weiter oben beschrieben eine oder mehrere Internet-Adressen, klicken Sie auf eine davon und ziehen Sie alle ausgewählten Internet-Adressen mit der Maus ins gewünschte Fenster.



Das Kontextmenü für die Sperrliste

Wie Sie bereits gesehen haben, können Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh auf eine Internet-Adresse in der Sperrliste klicken. Hierauf wird ein Kontextmenü geöffnet. Das Kontextmenü bietet mehrere Menüoptionen zur Auswahl an.



In Zwischenablage kopieren

Mit der Option „In Zwischenablage kopieren“ im Kontextmenü können Sie die Internet-Adresse in die Zwischenablage kopieren. Anschließend können Sie den Inhalt der Zwischenablage in ein Dokument jedes beliebigen Anwendungsprogramms einsetzen.

Bearbeiten…

Mit der Option „Bearbeiten“ im Kontextmenü können Sie einen Eintrag in der Sperrliste ändern. Siehe hierzu den Unterabschnitt **Ändern einer Internet-Adresse in der Sperrliste** weiter oben.

Entfernen…

Mit Hilfe der Option „Entfernen…“ im Kontextmenü können Sie einen Eintrag aus der Sperrliste entfernen. Siehe hierzu den Unterabschnitt **Löschen von Internet-Adressen aus der Sperrliste** weiter oben.

Zur vertrauenswürdigen Gruppe wechseln

Wenn Sie eine Internet-Adresse aus der Sperrliste in die vertrauenswürdige Gruppe verschieben wollen, müssen Sie die Menüoption „Zur vertrauenswürdigen Gruppe wechseln“ bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh aus dem Kontextmenü wählen.

Mit dieser Option im Kontextmenü können Sie eine Internet-Adresse aus der Sperrliste in die vertrauenswürdige Gruppe verschieben. Siehe hierzu den Unterabschnitt **Verschieben von Internet-Adressen aus der Sperrliste in die vertrauenswürdige Gruppe** weiter oben.

Domäneninformationen suchen

Wenn Sie die Menüoption „Domäneninformationen suchen“ aus dem Kontextmenü wählen, wird das Fenster „Whois“ von Intego NetBarrier X4 geöffnet und der Domänenname zur ausgewählten Internet-Adresse gesucht. Weitere Informationen hierzu finden Sie im Unterabschnitt **Whois** weiter unten.

Route suchen

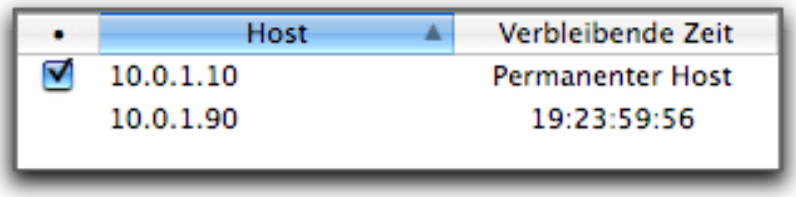
Wenn Sie die Menüoption „Domäneninformationen suchen“ aus dem Kontextmenü wählen, wird das Fenster „Whois“ von Intego NetBarrier X4 geöffnet und der Domänenname zur ausgewählten Internet-Adresse gesucht. Weitere Informationen hierzu finden Sie im Unterabschnitt **Traceroute** weiter unten.

Vertrauenswürdige Gruppe

Die Funktion „Vertrauenswürdige Gruppe“ ermöglicht es Ihnen, Internet-Adresse von Computern, die Sie als nicht feindlich gesinnt betrachten, in eine Liste vertrauenswürdiger Computer aufzunehmen. Wenn ein Computer mit einer der in dieser Liste enthaltenen Internet-Adresse versucht, eine Verbindung mit Ihrem Computer herzustellen (um beispielsweise eine Ping-Anfrage zu senden), wird dies nicht als Eindringversuch betrachtet. Die vertrauenswürdige Gruppe kann als das Gegenteil der Sperrliste betrachtet werden. Die Sperrliste enthält die Internet-Adressen potenzieller „Feinde“ und die vertrauenswürdige Gruppe die Internet-Adressen von „Freunden“. In die vertrauenswürdige Gruppe können Sie die Internet-Adressen von Computern in Ihrem lokalen Netzwerk oder von Computern im Internet aufnehmen, bei denen Sie sicher sind, dass sie nicht versuchen werden, Ihren Computer zu attackieren. Die Internet-Adressen in der vertrauenswürdigen Gruppe werden von der Funktion „Antivandalismus“ von Intego NetBarrier X4 nicht gesperrt, sodass auch keine Warnmeldungen ausgegeben werden, wenn einer dieser Computer versucht, eine Verbindung mit Ihrem Computer herzustellen. Allerdings gelten auch für die Computer der vertrauenswürdigen Gruppe alle aktiven Firewall-Regeln.

Informationen über die vertrauenswürdige Gruppe

Auf der Registerkarte „Vertrauenswürdige Gruppe“ werden die IP-Adressen von Computern angezeigt, die derzeit als vertrauenswürdig betrachtet werden.



Host

Die IP-Nummer des „freundlichen“ Computers.

Verbleibende Zeit

Dies ist die Zeitdauer (Verweildauer), worüber die Internet-Adresse eines „freundlichen“ Computers in der vertrauenswürdigen Gruppe gespeichert bleibt.

Andere Informationen über die vertrauenswürdige Gruppe

Wenn Sie einmal auf eine Internet-Adresse in der vertrauenswürdigen Gruppe klicken, werden in der rechten Hälfte der Registerkarte „Vertrauenswürdige Gruppe“ weitere Informationen angezeigt.

Host: 10.0.1.10
Gesamtzeit: Permanenter Host
Ankunft: 31.01.06, 10:09:43
Anmerkung: Dieser URL wurde in die Sperrliste aufgenommen wegen es versuchte, Ihren Computer mit Ping-Überflutung anzugreifen.

Host

An der Oberseite dieses Bereichs wird die IP-Nummer des „freundlichen“ Computers angezeigt. Wenn Sie auf die Schaltfläche zum Überprüfen der DNS klicken (das ?), können Sie zwischen der numerischen IP-Adresse und dem aktuellen Domänennamen eines befreundeten Computers hin- und herschalten, sofern es einen gibt. Sie können sich diese Adresse in großer Schrift anzeigen lassen. Verschieben Sie hierzu den Mauszeiger über das Etikett „Host“, bis es hervorgehoben dargestellt wird, klicken Sie mit der Maus darauf und wählen Sie aus dem Kontextmenü die Option „Große Schrift“.

Gesamtzeit

Dies ist der Zeitraum, über den die IP-Adresse eines „freundlichen“ Computers in der vertrauenswürdigen Gruppe gespeichert bleibt. Wenn Sie auf „Gesamtzeit“ klicken, können Sie sich den verbleibenden Zeitraum anzeigen

lassen, über den die Adresse noch in der Sperrliste gespeichert wird. Wenn Sie auf „Verbleibende Zeit“ klicken, wird Ihnen der bisher abgelaufene Zeitraum angezeigt. So erfahren Sie, wie lange die Adresse bereits in der Sperrliste gespeichert ist. Wenn Sie auf „Abgelaufene Zeit“ klicken, wird Ihnen noch einmal die Gesamtzeit angezeigt.

Ankunft

Im Abschnitt „Ankunft“ erfahren Sie, wann die Adresse vertrauenswürdigen Gruppe hinzugefügt wurde.

Start

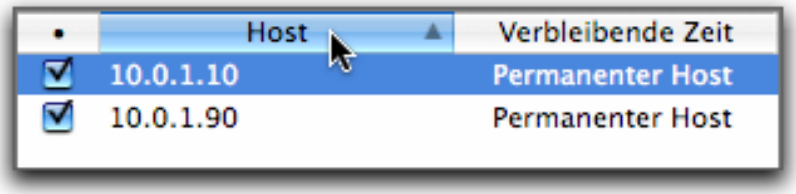
Im Abschnitt „Start“ erfahren Sie, wann die Adresse aus der vertrauenswürdigen Gruppe entfernt wird. Sie können diesen Zeitpunkt ändern, indem Sie den Mauszeiger über das Etikett „Start“ ziehen, bis es hervorgehoben wird. Dann klicken Sie darauf, wählen die Menüoption „Hinzufügen“ oder „Entfernen“ und wählen anschließend den Zeitraum aus, um den Sie die Gesamtzeit verlängern oder verkürzen wollen.

ANMERKUNG:

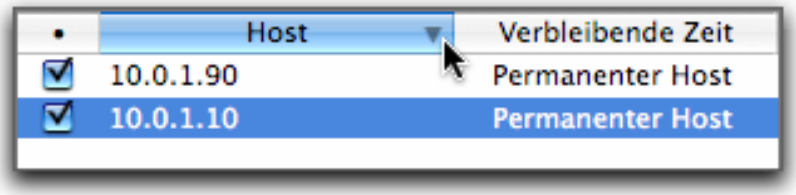
Im Textfeld in der unteren Hälfte dieses Abschnitts werden Anmerkungen angezeigt, die Sie zu der betreffenden IP-Adresse in die Liste der vertrauenswürdigen Computer eingegeben haben. Weitere Informationen über das Eingeben oder Hinzufügen von Anmerkungen zu einem Eintrag in der vertrauenswürdigen Gruppe finden Sie weiter unten.

Ändern der Listenanzeige

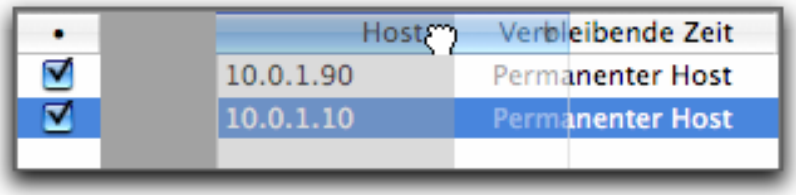
Sie können den Inhalt der vertrauenswürdigen Gruppe nach Spalteninhalten sortieren, indem Sie auf die Spaltenüberschrift klicken.



Durch Klicken aufs Sortierdreieck rechts neben der aktivierten Spaltenüberschrift können Sie die Sortierreihenfolge von auf- in absteigend ändern.



Sie können auch die Reihenfolge der Spalten ändern. Klicken Sie hierzu in die Überschrift der gewünschten Spalte, halten Sie die Maustaste gedrückt und ziehen Sie die Überschrift in die gewünschte Position. Lassen Sie die Maustaste wieder los.

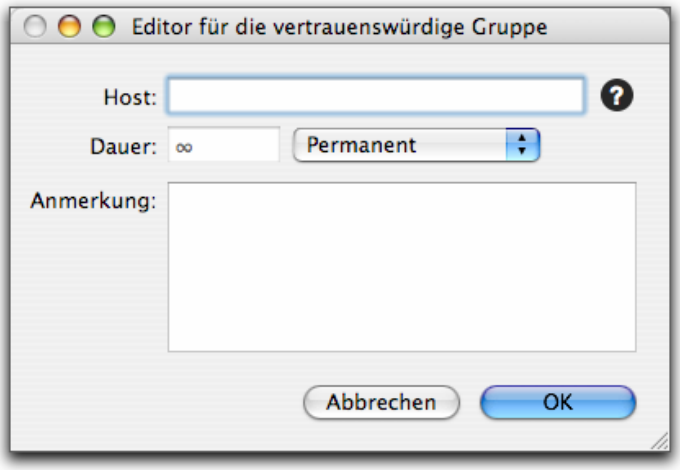


Hinzufügen von Internet-Adressen zur vertrauenswürdige Gruppe

Internet-Adressen können auf drei unterschiedliche Arten in die vertrauenswürdige Gruppe aufgenommen werden. Die erste Möglichkeit besteht darin, eine IP-Adresse aus dem Protokollfenster zu wählen und dann im Kontextmenü die Option „Zur vertrauenswürdigen Gruppe hinzufügen“ zu wählen. Weitere Informationen hierzu finden Sie im Unterabschnitt **Kontextmenü des Protokollfensters** weiter oben.

Eine Internet-Adresse kann auch mit Hilfe des Kontextmenüs aus der Sperrliste in die vertrauenswürdige Gruppe verschoben werden. Siehe hierzu den Unterabschnitt **Verschieben von Internet-Adressen aus der Sperrliste in die vertrauenswürdige Gruppe** weiter oben.

Sie können Internet-Adressen auch manuell in die vertrauenswürdige Gruppe aufnehmen. Klicken Sie hierzu auf die Schaltfläche „+“ in der unteren linken Ecke des Fensters. Hierauf wird das Fenster „Editor für die vertrauenswürdige Gruppe“ geöffnet.

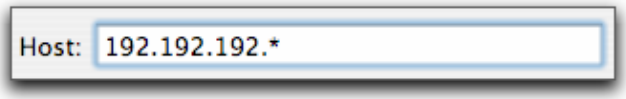


Geben Sie ins Feld „Host:“ die IP-Adresse eines Computers ein. Wählen Sie, über welchen Zeitraum diese in der vertrauenswürdigen Gruppe gespeichert bleiben soll,

indem Sie ins Feld „Dauer:“ eine entsprechende Zahl eingeben. Die Zeiteinheit können Sie aus dem Popup-Menü wählen. Wenn Sie die numerische IP-Adresse des anderen Computers, die Sie in die Sperrliste aufnehmen wollen, nicht kennen, müssen Sie seinen Domänennamen eingeben und auf die Schaltfläche mit dem Fragezeichen (**?**) klicken. Intego NetBarrier X4 fragt nun den DNS-Server Ihres ISP (Internet Service Provider = Internet-Dienstleister) an und trägt die korrekte IP-Nummer ins Feld ein. Ins Feld „Anmerkung:“ können Sie auch Anmerkungen wie z.B. den Grund für die Aufnahme der Internet-Adresse in die vertrauenswürdige Gruppe eingeben. Wenn Sie keine Internet-Adresse zur vertrauenswürdigen Gruppe hinzufügen wollen, müssen Sie nur auf die Schaltfläche „Abbrechen“ klicken.

Verwenden von Platzhalterzeichen in der vertrauenswürdigen Gruppe

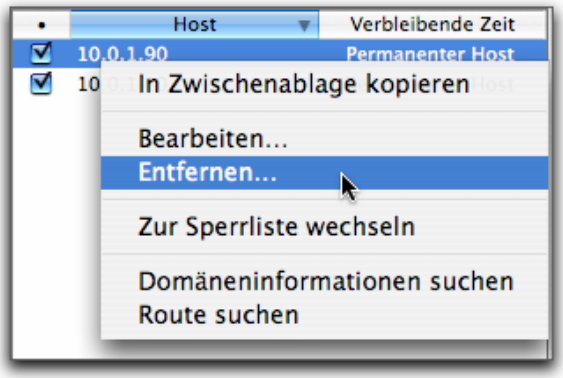
Sie können in IP-Nummern Platzhalterzeichen verwenden, um ganze Bereiche von IP-Nummern freizugeben. Geben Sie hierzu den ersten Teil einer IP-Nummer und dann eines oder mehrere Sternchen (*) ein: 192.*.*.*, 192.192.*.* oder 192.192.192.*. Hierdurch werden alle IP-Nummern freigegeben, in denen die eingegebenen Ziffern enthalten sind. Jedes Sternchen kann für eine beliebige Ziffer stehen.



Löschen von Internet-Adressen aus der vertrauenswürdigen Gruppe

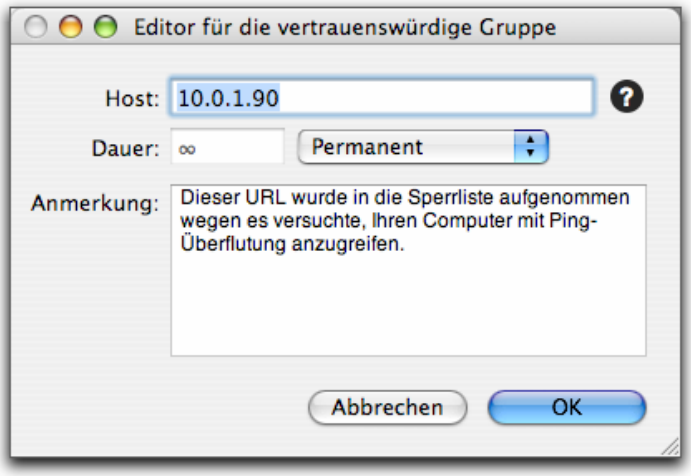
Wenn Sie eine Internet-Adresse aus der vertrauenswürdigen Gruppe löschen wollen, müssen Sie einmal auf die betreffende Internet-Adresse und dann auf die Schaltfläche „Entfernen“ klicken. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie die Internet-Adresse wirklich löschen wollen. Klicken Sie dann auf die Schaltfläche „Entfernen“. Die Internet-Adresse ist nun gelöscht. Wenn Sie die Internet-Adresse nicht löschen wollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken. Sie können mehrere nacheinander in der Liste angezeigte Internet-Adressen wählen, indem Sie auf eine dieser Internet-Adressen und dann bei gedrückter Umschalttaste auf die letzte der gewünschten Internet-Adressen klicken. Bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh können Sie auch Internet-Adressen auswählen, die nicht nacheinander in der Liste angezeigt werden.

Sie können eine Internet-Adresse auch aus der vertrauenswürdigen Gruppe löschen, indem Sie die Taste „ctrl“ in der Tastatur Ihres Macintosh gedrückt halten, auf die betreffende Internet-Adresse klicken und dann aus dem Kontextmenü die Option „Entfernen…“ wählen. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie die Internet-Adresse wirklich löschen wollen. Klicken Sie dann auf die Schaltfläche „Entfernen“. Die Internet-Adresse ist nun gelöscht. Wenn Sie die Internet-Adresse nicht löschen wollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.



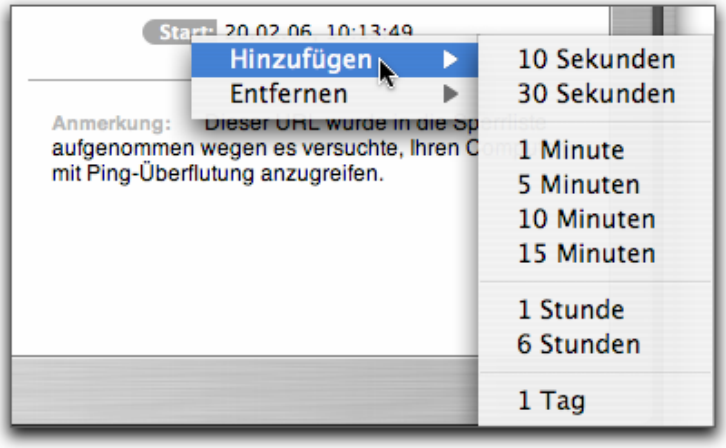
Ändern einer Internet-Adresse in der vertrauenswürdigen Gruppe

Wenn Sie eine Adresse in der vertrauenswürdigen Gruppe bearbeiten möchten, klicken Sie einmal auf die entsprechende Adresse und dann auf die Schaltfläche mit dem Bleistift auf der unteren linken Seite des Fensterabschnitts. (Sie können auch auf die Adresse doppelklicken oder bei gedrückter Steuerungstaste auf die Adresse klicken und anschließend „Bearbeiten…“ auswählen.)



Nun wird das Fenster „Editor für vertrauenswürdige Gruppe“ geöffnet, in dem Sie die IP-Adresse, Anmerkungen und die Verweildauer der IP-Adresse in der vertrauenswürdigen Gruppe ändern können. Um die Änderungen wirksam werden zu lassen, müssen Sie auf die Schaltfläche „OK“ klicken. Wenn die Änderungen nicht wirksam werden sollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.

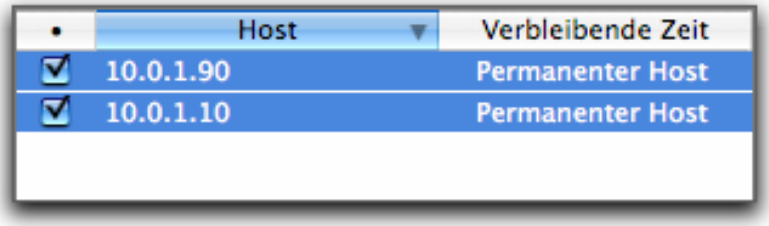
Sie können auch das Kontextmenü dazu verwenden, um die Verweildauer der Internet-Adresse in der vertrauenswürdigen Gruppe zu ändern. Verschieben Sie hierzu den Mauszeiger über das Etikett „Dauer“ in der vertrauenswürdigen Gruppe, bis es hervorgehoben dargestellt wird. Klicken Sie auf dieses Etikett und wählen Sie dann die Menüoption „Hinzufügen“ oder „Entfernen“. Wählen Sie dann einen Zeitraum aus dem Popup-Menü.



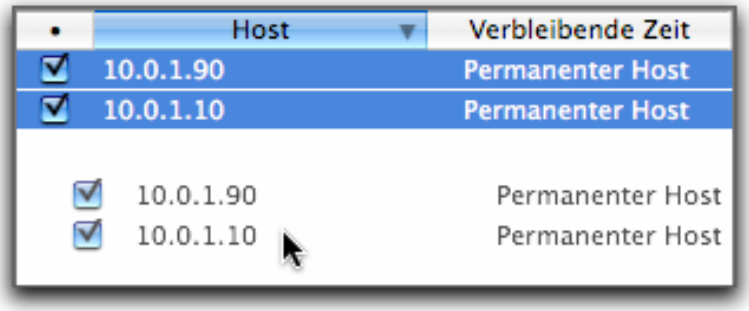
Wählen Sie die Zeit, um die Sie die Verweildauer der Internet-Adresse in der vertrauenswürdigen Gruppe verlängern oder verkürzen wollen. Diese Zeit wird sofort zur bisherigen Verweildauer addiert oder von dieser subtrahiert.

Kopieren von Internet-Adressen aus der vertrauenswürdigen Gruppe

Sie können Internet-Adressen aus der vertrauenswürdigen Gruppe wählen und in die Zwischenablage kopieren, um sie dann in ein Dokument eines anderen Anwendungsprogramms einzusetzen. Klicken Sie hierzu auf eine Zeile in der vertrauenswürdigen Gruppe und kopieren Sie dann die Internet-Adresse in die Zwischenablage. Sie können mehrere nacheinander in der Liste angezeigte Internet-Adressen wählen, indem Sie auf eine dieser Internet-Adressen klicken und dann bei gedrückter Umschalttaste auf die letzte der gewünschten Internet-Adressen klicken. Bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh können Sie auch Internet-Adressen auswählen, die nicht nacheinander in der Liste angezeigt werden.

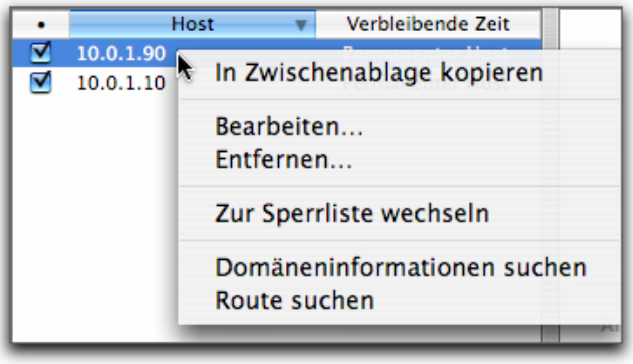


Sie können gewählte Internet-Adressen ins Fenster eines anderen Anwendungsprogramms ziehen und dort ablegen. Wählen Sie wie weiter oben beschrieben eine oder mehrere Internet-Adressen, klicken Sie auf eine davon und ziehen Sie alle ausgewählten Internet-Adressen mit der Maus ins gewünschte Fenster.



Das Kontextmenü für die vertrauenswürdige Gruppe

Wie Sie bereits gesehen haben, können Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh auf eine Internet-Adresse in der vertrauenswürdigen Gruppe klicken, worauf ein Kontextmenü geöffnet wird. Das Kontextmenü bietet mehrere Menüoptionen zur Auswahl an.



In Zwischenablage kopieren

Mit der Option „In Zwischenablage kopieren“ im Kontextmenü können Sie die Internet-Adresse in die Zwischenablage kopieren. Anschließend können Sie den Inhalt der Zwischenablage in ein Dokument jedes beliebigen Anwendungsprogramms einsetzen.

Bearbeiten…

Mit der Option „Bearbeiten…“ im Kontextmenü können Sie den Eintrag in der vertrauenswürdigen Gruppe ändern. Weitere Informationen hierzu finden Sie im Unterabschnitt **Ändern einer Internet-Adresse in der vertrauenswürdigen Gruppe** weiter oben.

Entfernen…

Mit der Option „Entfernen…“ im Kontextmenü können Sie die Internet-Adresse aus der vertrauenswürdigen Gruppe löschen. Weitere Informationen hierzu finden Sie im Unterabschnitt **Löschen von Internet-Adressen aus der vertrauenswürdigen Gruppe** weiter oben.

Zur Sperrliste wechseln

Mit dieser Option im Kontextmenü können Sie eine IP-Adresse aus der vertrauenswürdigen Gruppe in die Sperrliste verschieben.

Domäneninformationen suchen

Wenn Sie die Menüoption „Domäneninformationen suchen“ aus dem Kontextmenü wählen, wird das Fenster „Whois“ von Intego NetBarrier X4 geöffnet und der Domänenname zur ausgewählten Internet-Adresse gesucht. Weitere Informationen hierzu finden Sie im Unterabschnitt **Whois** weiter unten.

Route suchen

Wenn Sie die Menüoption „Domäneninformationen suchen“ aus dem Kontextmenü wählen, wird das Fenster „Whois“ von Intego NetBarrier X4 geöffnet und der Domänenname zur ausgewählten Internet-Adresse gesucht. Weitere Informationen hierzu finden Sie im Unterabschnitt **Traceroute** weiter unten.

Anti-Spyware

Intego NetBarrier X4 ermöglicht es Ihnen, festzulegen, welche Programme aufs Internet und/oder auf Ihr lokales Netzwerk zugreifen dürfen. Auch wenn Ihre Firewall-Einstellungen den allgemeinen Zugriff auf Netzwerke zulassen, ermöglichen es Ihnen die Optionen auf der Registerkarte „Anti-Spyware“, festzulegen, wie Intego NetBarrier X4 reagieren soll, wenn bestimmte Anwendungsprogramme versuchen, auf ein Netzwerk zuzugreifen. Dies ermöglicht ihnen zweierlei:

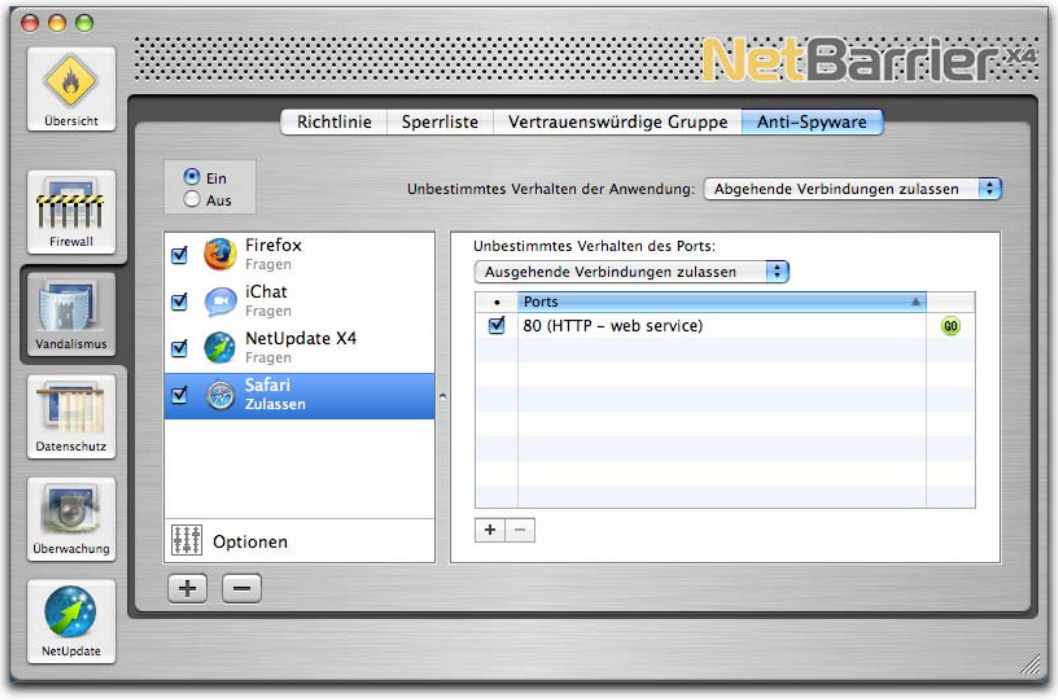
- Wenn Sie wollen, dass bestimmte Anwendungsprogramme nicht aufs Netzwerk zugreifen können, können Sie dies mit Hilfe der entsprechenden Optionen auf der Registerkarte „Anwendungsprogramme“ sperren.
- Wenn ein Anwendungsprogramm versucht, eine Verbindung mit einem Netzwerk herzustellen, ohne dass Sie hiervon etwas erfahren, blockiert Intego NetBarrier X4 diesen Versuch, gibt eine Warnmeldung aus und fordert Sie auf, diesen Zugriff zuzulassen oder zu verweigern.

Auf der Festplatte Ihres Computers befinden sich viele Anwendungsprogramme, die aufs Internet oder auf andere Netzwerk zugreifen: Webbrowser, E-Mail-Programme, FTP-Programme für den Dateitransfer, Dialogprogramme für IRC, ICQ usw. Viele dieser Programme sind dafür vorgesehen, übers Internet zu kommunizieren, während andere heimlich versuchen, eine Verbindung mit dem Internet herzustellen. In manchen Fällen versuchen dieser Programme, automatisch nach neuen Versionen von Software zu suchen. Eines dieser Programme ist beispielsweise Intego NetUpdate. Auch wenn Sie derartige Programme so konfiguriert haben, dass sie in bestimmten Zeitintervallen eine Verbindung mit dem Internet herstellen, werden Sie über den Umfang des im Hintergrund laufenden Datenverkehrs überrascht sein. Es kann jedoch auch vorkommen, dass Programme eine Netzwerkverbindung herstellen, ohne Sie darüber zu informieren, um beispielsweise die Seriennummer eines auf Ihrem Computer installierten Anwendungsprogramms zu versenden, persönliche Daten über Sie zu sammeln und

heimlich auf einen Server hochzuladen, oder ein Hintertürchen in Ihrem Computersystem zu öffnen, sodass Hacker oder Vandalen Zugriff auf Ihren Computer erhalten.

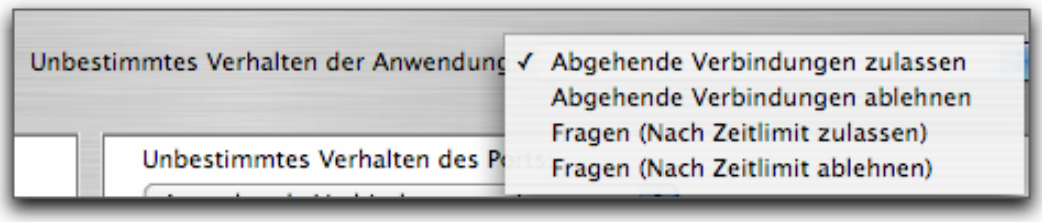
Verwenden der Registerkarte „Anti-Spyware“

Auf der Registerkarte „Anti-Spyware" von Intego NetBarrier X4 können Sie festlegen, wie die Software reagieren soll, wenn ein neues Anwendungsprogramm versucht, eine Verbindung mit dem Internet und einem anderen Netzwerk herzustellen.



Um das Sperren von Anwendungsprogrammen zu aktivieren, müssen Sie aufs runde Optionsfeld „Ein“ klicken.

Wählen Sie anschließend eine der vier Verhaltensoptionen für nicht definierte Anwendungsprogramme:



Abgehende Verbindungen zulassen

Wenn Sie diese Option wählen, ermöglicht Intego NetBarrier X4 allen Anwendungsprogrammen den Zugriff aufs Internet und andere Netzwerke. Von Ihnen definierte Firewall-Regeln, womit Sie den Zugriff auf bestimmte Ports zugelassen oder gesperrt haben, bleiben jedoch in Kraft. Wenn beispielsweise ein FTP-Programm versucht, eine Verbindung mit einem Server herzustellen, wird der Internet-Zugriff durch dieses Anwendungsprogramm nicht von Intego NetBarrier X4 gesperrt. Wenn Sie aber eine Firewall-Regel definiert haben, durch die der Zugriff auf den Port 20 (den standardmäßigen FTP-Port) gesperrt wird, so wird der Datentransfer blockiert. Wenn das FTP-Programm versucht, eine Verbindung über einen anderen Port herzustellen, wird es nicht blockiert.

Abgehende Verbindungen ablehnen

Wenn dieses runde Optionsfeld markiert ist, ermöglicht Intego NetBarrier X4 allen Anwendungsprogrammen den Zugriff aufs Internet und andere Netzwerke. Hierdurch werden alle von Ihnen definierten Firewall-Regeln außer Kraft gesetzt.

Fragen (Nach Zeitlimit zulassen)

Wenn Sie das runde Optionsfeld „Fragen“ markieren, werden Sie von Intego NetBarrier X4 bei jedem Versuch eines Anwendungsprogramms, eine Verbindung herzustellen, gefragt, ob Sie dies zulassen oder verweigern wollen.

Wenn Sie nicht innerhalb eines Zeitlimits von 90 Sekunden antworten, wird dem Anwendungsprogramm der Zugriff auf das Internet für dieses eine Mal gestattet.

Fragen (Nach Zeitlimit ablehnen)

Wenn Sie das runde Optionsfeld „Fragen“ markieren, werden Sie von Intego NetBarrier X4 bei jedem Versuch eines Anwendungsprogramms, eine Verbindung herzustellen, gefragt, ob Sie dies zulassen oder verweigern wollen. Wenn Sie nicht innerhalb eines Zeitlimits von 90 Sekunden antworten, wird dem Anwendungsprogramm der Zugriff auf das Internet für dieses eine Mal verweigert.

Optionen

Mit der Schaltfläche „Optionen“ in der unteren linken Ecke des Fensterabschnitts „Anti-Spyware“ können Sie einige allgemeine Einstellungen für Anti-Spyware konfigurieren.

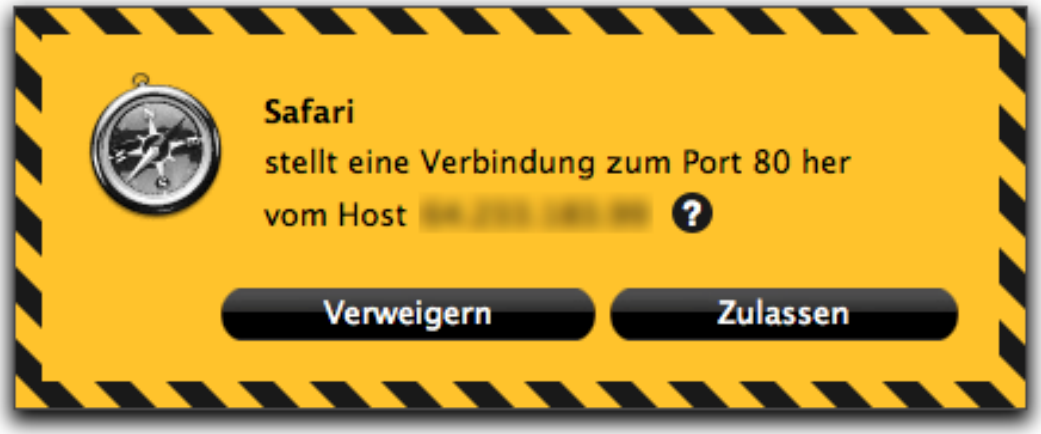
Filterung

Systemprozessen vertrauen

Viele Komponenten von Mac OS X greifen unbemerkt aufs Internet oder aufs lokale Netzwerk zu. Bei diesen Systemprozessen kann es sich um Druckdienste, Dienste für die Auflösung von Domänennamen oder Prozesse handeln, die einen Server auf neue Versionen von Software prüfen oder die interne Uhr Ihres Computers mit einer Normalweituhr synchronisieren. Wenn Sie diesen Prozessen vertrauen und nicht jedes Mal gefragt werden wollen, wenn diese eine Verbindung mit dem Internet oder dem lokalen Netzwerk herstellen wollen, müssen Sie das Kontrollkästchen „Systemprozessen vertrauen“ markieren.

Alarm

Wenn Sie festgelegt haben, dass eine Warnmeldung ausgegeben werden soll, wenn ein Anwendungsprogrammen versucht, aufs Internet oder ein anderes Netzwerk zuzugreifen, wird ein Fenster mit einer Warnmeldung geöffnet.



Durch diese Warnmeldung wird Ihnen mitgeteilt, dass ein Anwendungsprogramm versucht hat, eine Verbindung mit einem Computer mit einer bestimmten IP-Adresse herzustellen. Intego NetBarrier X4 stellt Ihnen mehrere Schaltflächen zur Verfügung, mit denen Sie festlegen können, wie NetBarrier X4 in diesem Fall reagieren soll.

Verweigern

Wenn Sie auf diese Schaltfläche klicken, sperrt Intego NetBarrier X4 den Netzwerkzugriff für dieses Anwendungsprogramm. Wenn Sie die Optionstaste („alt“) drücken, wechselt die Schaltfläche „Verweigern“ auf „Einmalig nicht zulassen“. So können Sie den Zugriff für dieses eine Mal verweigern. Wenn das Anwendungsprogramm das nächste Mal versucht, eine Verbindung zum Netzwerk aufzubauen, werden Sie erneut gewarnt.

Zulassen

Wenn Sie diese Option wählen, erlaubt Intego NetBarrier X4 diesem Anwendungsprogramm den Netzwerkzugriff dieses Mal und in Zukunft – vorausgesetzt, das Anwendungsprogramm verwendet den Port, den Sie aktuell zulassen. Wenn das Anwendungsprogramm künftig einen anderen Port verwendet, zeigt NetBarrier X4 eine neue Warnmeldung an. Sie können den Netzwerkzugriff daraufhin zulassen oder verweigern. Wenn Sie die Optionstaste („alt“) drücken, wechselt die Schaltfläche „Zulassen“ auf „Einmalig zulassen“. So können Sie den Zugriff für dieses eine Mal erlauben. Wenn das Anwendungsprogramm das nächste Mal versucht, eine Verbindung zum Netzwerk aufzubauen, werden Sie erneut gewarnt.

Wenn Sie nicht wissen, welches Anwendungsprogramm eine Verbindung mit dem Internet- oder dem Netzwerk aufbauen möchte, können Sie den Mauszeiger über den Namen des Programms bewegen, bis das Etikett hervorgehoben wird. So wird ein Fenster im Finder geöffnet, in dem Ihnen der Speicherort des Programms auf Ihrem Computer angezeigt wird.

Eventuell möchten Sie auch den Namen der Domäne wissen, die im Warnfenster angezeigt wird. Wenn Sie auf die Schaltfläche zum Überprüfen der DNS klicken (das ?), können Sie zwischen der numerischen IP-Adresse und dem aktuellen Domänennamen des Computers hin- und herschalten, sofern es einen gibt.

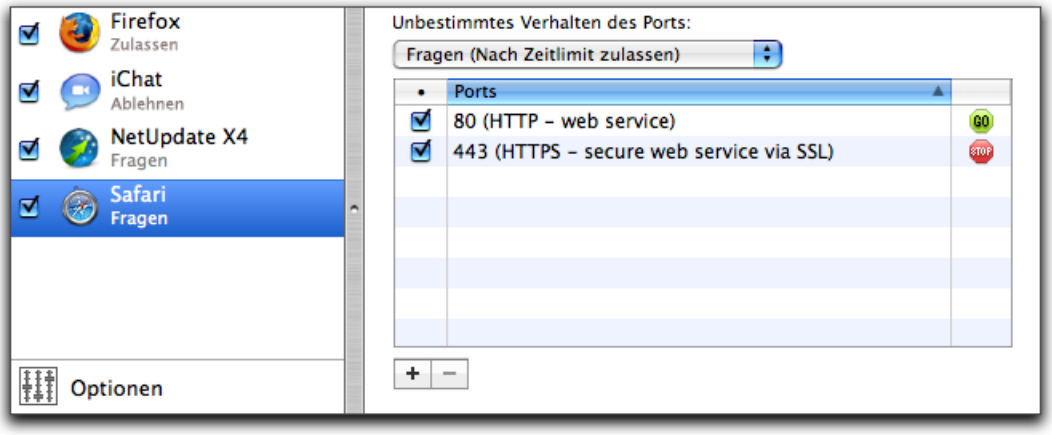
Zusätzlich zum oder anstelle des Fensters mit der Warnmeldung können Sie die Warnmeldung auch als gesprochenen Text erhalten und/oder einen Warnton abspielen lassen. Markieren Sie das jeweilige Kästchen für die Warnoption, die Sie aktivieren möchten.

Wenn Sie die Option „Rückmeldung über abgelehnte Verbindungen“ auswählen, werden Sie informiert, wenn eine von Ihnen abgelehnte Verbindung versucht, auf ein

Netzwerk zuzugreifen. Sie können sich entweder durch ein transparentes Fenster (wie unten dargestellt) und/oder einen Sound warnen lassen.

Ändern von Einstellungen für Anwendungsprogramme

Nachdem Sie festgelegt haben, dass ein bestimmtes Anwendungsprogramm aufs Internet oder ein anderes Netzwerk zugreifen darf oder gesperrt ist, können Sie diese Einstellungen jederzeit ändern. Dieses Fenster zeigt eine Liste von Anwendungsprogrammen, für die Sie nach Aufforderung durch Intego NetBarrier X4 festgelegt haben, ob der Netzwerkzugriff zugelassen oder verweigert werden soll oder ob Sie noch einmal gefragt werden möchten. (Wenn Sie den Netzwerkzugriff für ein Anwendungsprogramm nur einmal freigegeben haben, erscheint das entsprechende Anwendungsprogramm nicht in dieser Liste.)



Wenn Sie auf ein bestimmtes Programm klicken, zeigt das Fenster die Ports an, die Sie zugelassen oder verweigert haben.

Diese Portliste besteht aus drei Spalten:

In der ersten Spalte, die mehrere Kontrollkästchen enthält, wird das fürs Programm derzeit aktivierte Portverhalten angezeigt. Wenn das Kästchen neben einem Port markiert ist, wurde das von Ihnen festgelegte Verhalten aktiviert.

Wenn Sie dieses Verhalten deaktivieren möchten, müssen Sie das Häkchen aus dem Kästchen entfernen. Sie können das Verhalten später erneut aktivieren, indem Sie das Kästchen wieder markieren.

Die zweite Spalte mit der Überschrift „Ports“ zeigt Ihnen Informationen über die Ports an, die das Programm für den Netzwerkzugriff verwendet. Hier erfahren Sie die Port-Nummer und manchmal auch das verwendete Protokoll sowie eine kurze Beschreibung. Sie können eine Port-Nummer oder eine Reihe von Port-Nummern hinzufügen, beispielsweise 110-123.

Die dritte Spalte zeigt eines von zwei Symbol an: Ein grünes Symbol mit dem Etikett „GO“, wodurch angezeigt wird, dass der Netzwerkzugriff erlaubt wurde oder ein rotes Symbol mit dem Etikett „STOP“, wodurch angezeigt wird, dass der Netzwerkzugriff gesperrt wurde.

Wenn Sie die Einstellung von „Zulassen“ in „Verweigern“ ändern möchten, klicken Sie einfach auf die grüne „GO“-Schaltfläche. Diese verwandelt sich dann in das rote „STOP“-Symbol. Auf die gleiche Weise können Sie von „STOP“ zu „GO“ wechseln.

Hinzufügen von Anwendungsprogrammen zur Anti-Spyware-Programmliste

Intego NetBarrier X4 ermöglicht es Ihnen, Anwendungsprogramme manuell zur Liste der angemeldeten Anwendungsprogramme hinzuzufügen. Danach können Sie festlegen, ob das jeweilige Anwendungsprogramm Netzwerkzugriff haben darf.

Klicken Sie auf die Schaltfläche „+“ in der unteren linken Ecke des Fensters, wenn Sie ein Programm hinzufügen möchten. Hierauf wird ein standardmäßiges Dialogfeld von Mac OS X geöffnet. Navigieren Sie zum Programm, das Sie hinzufügen möchten und klicken Sie dann auf „Hinzufügen“. Wenn Sie auf diese Weise ein Programm hinzufügen, erhält es den Status „Zulassen“. Alle Netzwerkzugriffe werden so für dieses Programm erlaubt. Wenn Sie diese Einstellung ändern möchten, klicken Sie auf eine der Optionen in der Liste „Unbestimmtes Verhalten der Ports“ (siehe „Ändern der Einstellungen für Anwendungsprogramme“ weiter oben).

Sie können Anwendungsprogramme auch in die Liste aufnehmen, indem Sie ihre Symbole auf die Registerkarte „Programme“ ziehen. Suchen Sie das gewünschte Anwendungsprogramm und ziehen Sie sein Symbol auf die Registerkarte „Programme“.

Löschen von Anwendungsprogrammen aus der Anti-Spyware-Programmliste

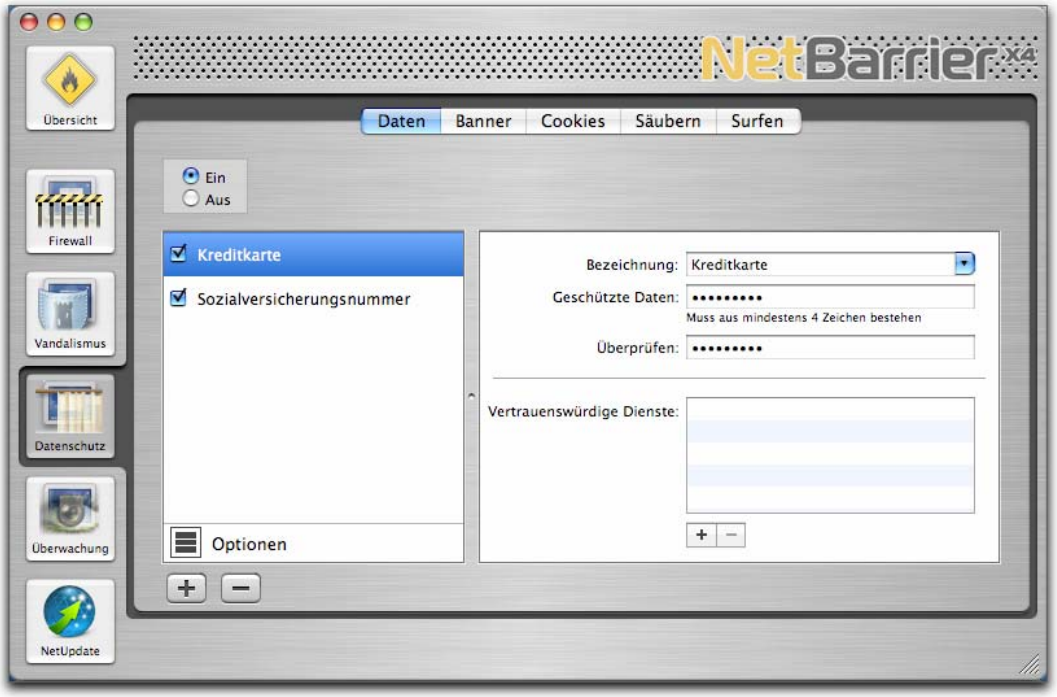
Wenn Sie eine Anwendung aus der Programmliste entfernen möchten, klicken Sie auf eines der Programme, um es auszuwählen. Klicken Sie anschließend auf die Schaltfläche „-“ in der unteren linken Ecke des Fensters. Dann wird Ihnen ein Fenster angezeigt, indem Sie bestätigen müssen, dass Sie dieses Programm tatsächlich aus der Liste entfernen möchten. Klicken Sie auf die Schaltfläche „Entfernen“, um es zu löschen, oder auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Anzeigen von Anwendungsprogrammen im Finder

Wenn Sie sehen wollen, wo sich ein in der Programmliste aufgeführtes Anwendungsprogramm auf der Festplatte befindet, müssen Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh auf den Namen des entsprechenden Anwendungsprogramms klicken. Nun wird ein Kontextmenü geöffnet. Wählen Sie die Menüoption „Im Finder anzeigen“. Nun wird ein Fenster im Finder geöffnet, in dem Ihnen der Speicherort des Anwendungsprogramms auf Ihrem Computer angezeigt wird.

Schutz persönlicher Daten

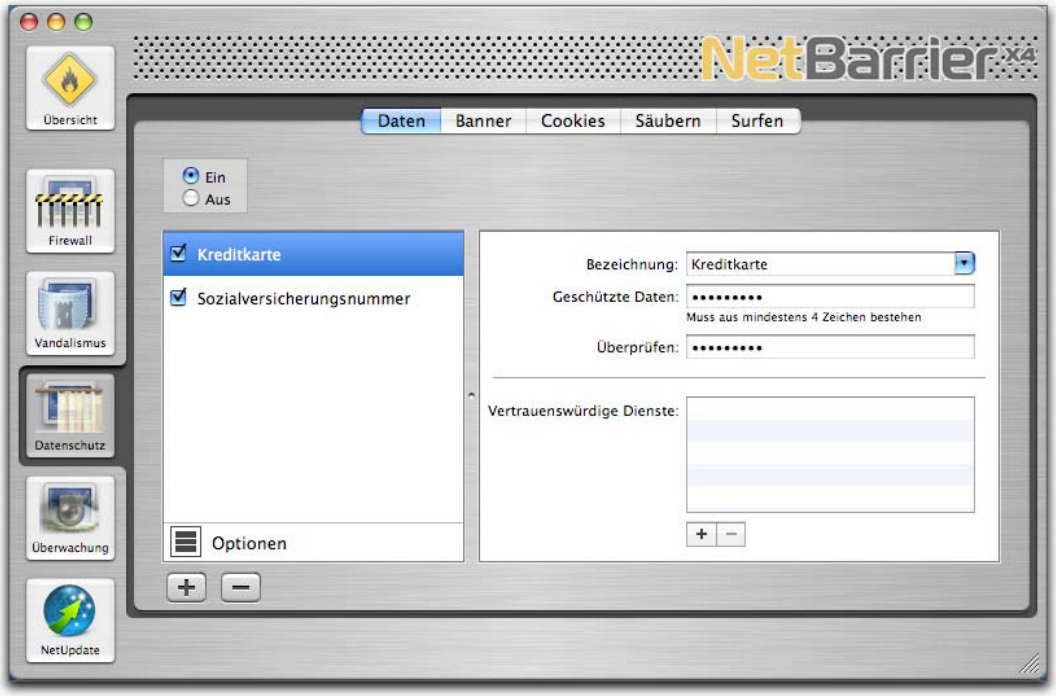
Intego NetBarrier X4 kann ein- und ausgehende Datenpakete filtern und nach bestimmten Datentypen suchen. In Intego NetBarrier X4 sind mehrere Filter integriert, um den Schutz Ihrer persönlichen Daten sicherzustellen und die Geschwindigkeit beim Surfen im World Wide Web zu erhöhen.



Datenfilter

Der Datenfilter von Intego NetBarrier X4 stellt sicher, dass sensible, auf Ihrem Computer gespeicherte Daten von diesem nicht über ein Netzwerk versandt werden können. Sie entscheiden selbst, welche Daten Ihren Computer nicht verlassen dürfen: Ihre Kreditkartennummer, Passwörter oder Schlüsselwörter aus vertraulichen Dokumenten usw. Der in Intego NetBarrier X4 integrierte Datenfilter prüft jedes ausgehende Datenpaket darauf, dass diese vertraulichen Daten nicht von Ihrem Computer gesendet werden. Hierdurch wird nicht nur sichergestellt, dass keine Dokumente versandt werden können, in denen diese vertraulichen Daten enthalten sind. Intego NetBarrier X4 macht es einem Eindringling auch unmöglich, diese sensiblen Daten zu „stehlen“.

Denken Sie daran: Wenn Ihr Computer in ein Netzwerk eingebunden ist und andere Benutzer über die Datei- und Druckerfreigabe auf Ihre Dateien zugreifen können, haben diese Benutzer selbstverständlich die Möglichkeit, Ihre Daten zu kopieren.



Funktion des Datenfilters

Der Datenfilter arbeitet einfach, aber effektiv. Alle Daten, die Sie geschützt haben wollen, werden als geschützte Daten bezeichnet. Wenn Ihr Computer Datenpakete in ein Netzwerk sendet (in ein lokales Netzwerk oder ins Internet), werden diese Datenpakete von Intego NetBarrier X4 daraufhin geprüft, ob es sich um geschützte Daten handelt. Wenn das Datenpaket geschützt ist, wird das Senden desselben gesperrt.

Anmerkung: Der Datenfilter filtert nur Datenpakete aus, in denen geschützte Daten enthalten sind. Welche Daten geschützt werden sollen, müssen Sie selbst definieren. Wenn Sie beispielsweise Ihre Kreditkartennummer schützen (siehe unten), verhindert Intego NetBarrier X4, dass sie von Ihrem Computer versandt wird. Wenn Sie Ihre Kreditkartennummer jedoch auf einer sicheren HTML-Seite mit Datenverschlüsselung eingeben, wird sie von Ihrem Webbrowser verschlüsselt, sodass die Datenpakete nicht mehr mit der geschützten Kreditkartennummer identisch sind. Der Versand Ihrer Kreditkartennummer kann in diesem Fall nicht von Intego NetBarrier X4 gesperrt werden. Das Gleiche gilt für codierte oder komprimierte Daten.

Aktivieren des Datenfilters

Bevor Intego NetBarrier X4 ausgehende Datenpakete auf geschützte Daten prüfen kann, muss der Datenfilter aktiviert sein. Klicken Sie hierzu aufs runde Optionsfeld „Ein“. Sie können den Datenfilter jederzeit abschalten, wenn Sie geschützte Daten vorübergehend versenden wollen, indem Sie aufs runde Optionsfeld „Aus“ klicken.

Zu schützende Daten

Der Datenfilter ist dafür vorgesehen, sensible Daten vor einem Versenden durch Ihren Computer zu schützen. Hierbei kann es sich um die unterschiedlichsten Daten handeln. Hier sind einige Beispiele:

Kreditkartennummern

Auch wenn Sie nicht wollen, dass Ihre Kreditkartennummer übers Internet per E-Mail oder an Website-Server versandt wird, haben Sie Ihre Kreditkartennummer vermutlich schon einmal per Fax versandt. Wenn Sie das Fax von Ihrem Computer aus versandt haben, wurde vorher ein Dokument (z.B. in Microsoft Word) erstellt, in dem Ihre Kreditkartennummer enthalten ist. Diese Datei könnte nun von einem Hacker kopiert werden. Geben Sie Ihre Kreditkartennummer einfach in die Filterliste ein, und sie kann nicht mehr von Ihrem Computer aus in ein Netzwerk gesendet werden.

Passwörter

Wenn Sie das Internet oder ein anderes Netzwerk nutzen, verwenden Sie höchstwahrscheinlich auch Passwörter, um Zugriff auf bestimmte HTML-Seite usw. zu erhalten. Je mehr Websites Sie besuchen, umso mehr Passwörter verwenden Sie vermutlich. Manche Benutzer speichern sogar Listen mit allen ihren Passwörtern auf ihren Computern. Geben Sie Ihre Passwörter einfach in die Filterliste ein, und sie können nicht mehr von Ihrem Computer aus in ein Netzwerk gesendet werden. Anmerkung: Wenn Sie Ihre Passwörter im Schlüsselbund von Mac OS X gespeichert haben, werden sie verschlüsselt, sodass ihr Versand nicht von NetBarrier X4 gesperrt werden muss.

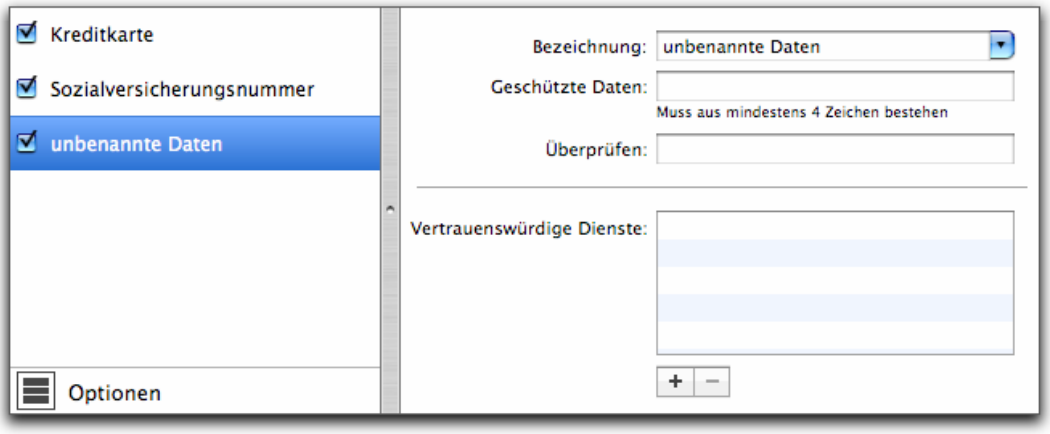
Andere sensible Informationen

Unter Umständen haben Sie auf Ihrem Computer Dokumente mit vertraulichen Daten über Projekte, Kunden, Verträge, technische Daten usw. gespeichert. Sie

können diese Dokumente vor dem „Diebstahl“ durch Hacker schützen, indem Sie darin enthaltene Begriffe wie Projekt- oder Kundennamen oder Schlüsselwörter in die Filterliste eingeben. Dadurch wir sichergestellt, dass Dateien, in denen diese Begriffe vorkommen, nicht über ein Netzwerk versandt werden können. Sie können auch den Versand von E-Mail-Adressen, Sozialversicherungsnummern, Telefonnummern usw. sperren.

Hinzufügen zu schützender Daten in die Filterliste

Klicken Sie auf die Schaltfläche „+“ in der unteren linken Ecke des Fensterabschnitts, wenn Sie dem Filter Daten hinzufügen möchten, die geschützt werden sollen. Daraufhin wird ein neuer Fensterabschnitt mit unbenannten Daten angezeigt.

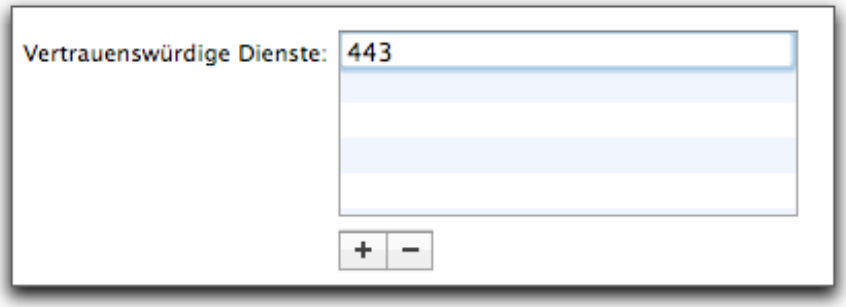


Geben Sie ins Feld „Bezeichnung:“ einen Namen für den neuen Filter ein. Aus dem Popup-Menü rechts von diesem Feld können Sie ein passendes Etikett wählen. Geben Sie dann den zu schützenden Text ins zweite Textfeld ein. Bei der Eingabe dieses Textes sehen Sie statt der eingegebenen Zeichen mittig stehende Punkte, sodass niemand sehen kann, was Sie eingeben. Den aktuellen Text müssen Sie dann noch einmal in das Bestätigungsfeld eingeben. Wenn die Eingabefelder für die zu schützenden Daten und die Bestätigung nicht übereinstimmen, wird ein Fenster eingeblendet, in dem Sie auf diesen Fehler hingewiesen werden. Sie können dann entweder die zu schützenden Daten noch einmal in beide Datenfelder eingeben oder auf die Schaltfläche „OK“ klicken. Wenn Sie auf „OK“ klicken, müssen Sie nur das Bestätigungsfeld neu ausfüllen.

Anmerkung: Sie müssen den Text exakt so eingeben, wie er in den entsprechenden Dokumenten enthalten ist. Beispielsweise kann eine Kreditkartennummer in einem

Dokument im Format ####-####-####-#### oder #### #### #### #### enthalten sein. Wenn Sie Ihre Kreditkartennummer nur im ersten Format eingeben, kann Intego NetBarrier X4 Ihre Kreditkartennummer nicht schützen, wenn sie in einem Dokument im zweiten Format enthalten ist. Achten Sie bei der Eingabe zu schützender Daten auch unbedingt auf korrekte Groß- und Kleinschreibweise. Wenn Sie ein Schlüsselwort wie z.B. einen Projektnamen eingeben wollen, müssen Sie dies in allen möglichen Varianten tun: Marktuntersuchung, MARKTUNTERSUCHUNG.

Im Abschnitt mit der Bezeichnung **Vertrauenswürdige Dienste** können Sie auswählen, dass Daten für alle bis auf die ausgewählten Diensten gesperrt werden sollen. Klicken Sie hierzu auf die Schaltfläche „+“. Geben Sie anschließend die Port-Nummer des Dienstes ein. Sie können eine Port-Nummer oder eine Reihe von Port-Nummer hinzufügen, beispielsweise 110-123. Diese Daten werden dann nur für diesen Dienst nicht gesperrt. Wenn Sie andere Dienste hinzufügen wollen, müssen Sie den vorstehend beschriebenen Vorgang wiederholen. Sie können beliebig viele Dienste hinzufügen.

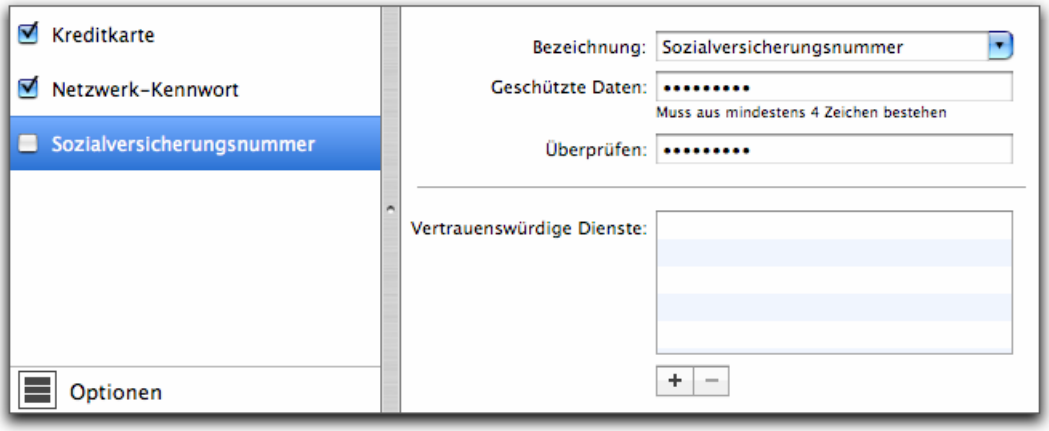


Sie können Dienste auch per Drag&Drop aus der Dienste-Bibliothek hinzufügen. Dies ist besonders dann hilfreich, wenn Sie die entsprechenden Port-Nummern nicht kennen, die Sie der Liste hinzufügen möchten. Gehen Sie zum Öffnen der Dienste-Bibliothek in den Abschnitt „Firewall“. Klicken Sie auf den Reiter „Allgemein“ und anschließend auf die Schaltfläche „Dienste-Bibliothek“ in der unteren rechten Ecke. Wählen Sie den gewünschten Dienst aus und ziehen Sie ihn in die Liste für vertrauenswürdige Dienste.

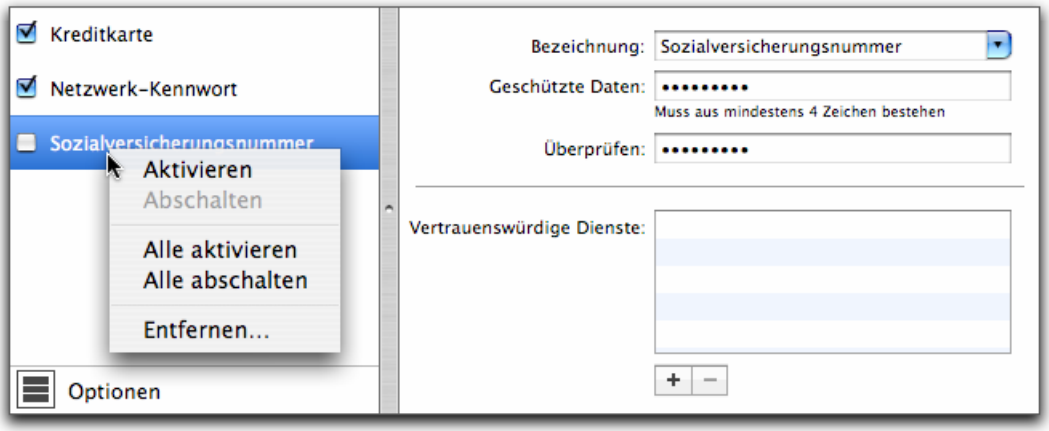
Sobald Sie diese Informationen vollständig eingegeben haben, werden Ihre Daten geschützt.

Aktivieren oder Abschalten des Schutzes von Daten

Jedes geschützte Objekt wird im Datenfenster in einer eigenen Zeile angezeigt. Mit Hilfe des Kontrollkästchens links von jeder Zeile können Sie den Filter fürs betreffende Objekt aktivieren oder abschalten. Wenn Sie ein neues Objekt hinzufügen, wird das Kontrollkästchen links davon automatisch markiert, wodurch angezeigt wird, dass der Filter für dieses Objekt aktiviert wurde. Wenn Sie geschützte Daten übers Internet oder ein lokales Netzwerk versenden wollen, müssen Sie die Markierung des Kontrollkästchens für dieses Objekt entfernen.



Sie können die Datenfilter für einzelne oder alle geschützten Daten aktivieren. Klicken Sie hierzu bei gedrückter Taste „ctrl“ auf der Tastatur Ihres Macintosh auf den Namen der gewünschten Objekte. Nun wird ein Kontextmenü geöffnet.



Wählen Sie die Menüoption „Aktivieren“ fürs gewünschte Objekt oder die Menüoption „Alle aktivieren“, um den Schutz für alle Objekte zu aktivieren.

Auf die gleiche Weise können Sie den Schutz für einzelne oder alle Objekte abschalten.

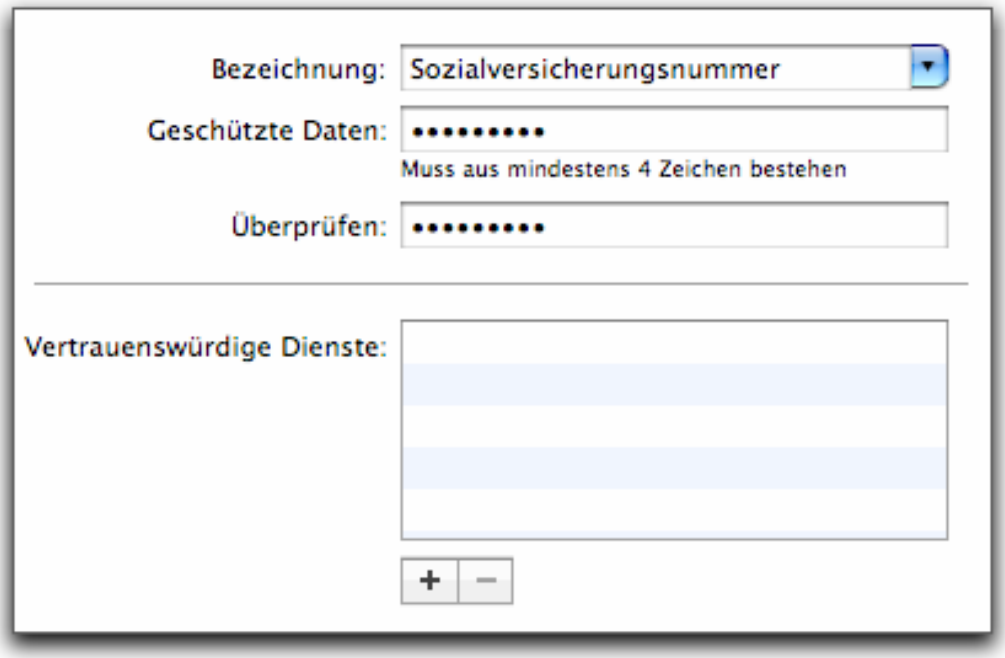
Löschen geschützter Daten aus der Liste geschützter Daten

Wenn Sie geschützte Daten aus der Liste löschen wollen, müssen Sie aufs gewünschte Objekt und dann auf „-“ klicken. Nun wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie die geschützten Daten wirklich aus der Liste löschen wollen. Klicken Sie dann auf die Schaltfläche „OK“. Die geschützten Daten werden nun aus der Liste gelöscht. Wenn Sie die geschützten Daten nicht aus der Liste löschen wollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.

Ändern der Eigenschaften von Objekten in der Liste geschützter Daten

Sie können die Eigenschaften von Objekten in der Liste geschützter Daten oder der damit in Zusammenhang stehenden Dienste ändern.

Wenn Sie die Eigenschaften eines Objekts in der Liste geschützter Daten ändern wollen, müssen Sie einmal auf den Namen des betreffenden Objekts klicken. Die geschützten Daten werden im rechten Fensterabschnitt angezeigt. Sie können dann alle gewünschten Änderungen daran vornehmen.



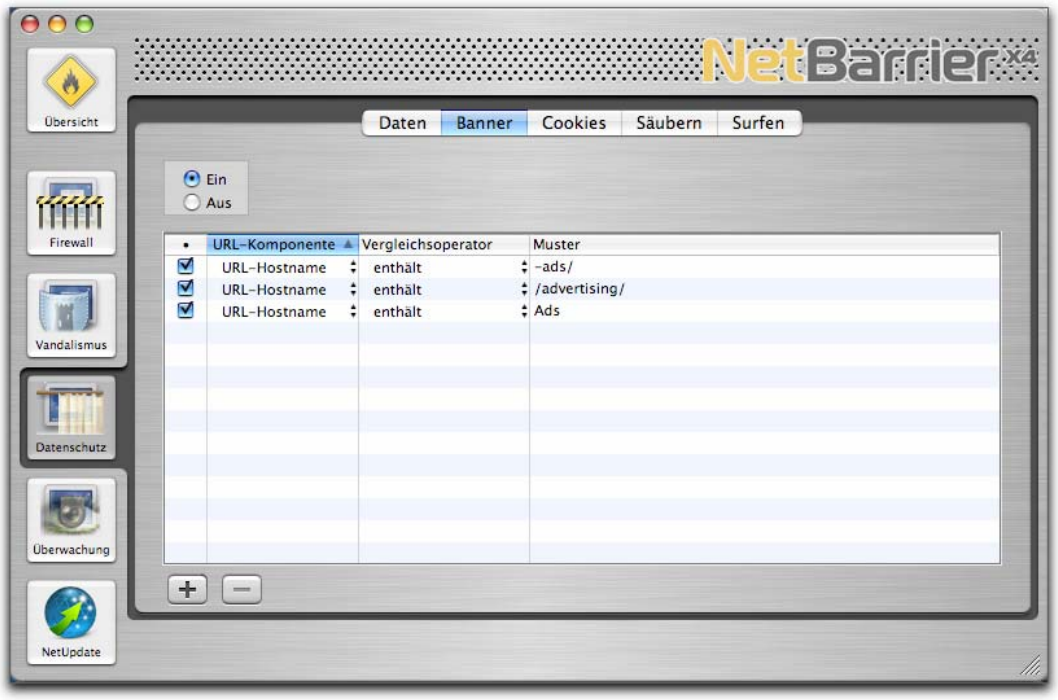
Filterwarnmeldungen

Wenn Intego NetBarrier X4 erkennt, dass Ihr Computer versucht, geschützte Daten über ein Netzwerk zu versenden, wird eine Warnmeldung angezeigt.

Diese Warnmeldung ähnelt anderen von Intego NetBarrier X4 ausgegebenen Warnmeldungen. Sie können die Warnmeldung ignorieren oder die Internet-Adresse des anderen Computers in die Sperrliste aufnehmen. Wenn Sie auf die Schaltfläche „Ignorieren“ klicken, ermöglicht Intego NetBarrier X4 es ihrem Computer, die Daten 10 Sekunden lang zu senden. Im Allgemeinen reicht diese Zeit aus, um eine Datei zu versenden. Wenn Sie auf die Schaltfläche „Sperrliste“ klicken, wird die Internet-Adresse des anderen Computers zur Sperrliste hinzugefügt.

Banner-Filter

Wenn Sie auf die Registerkarte „Banner“ klicken, wird das Fenster „Bannerfilter“ geöffnet. In diesem Fenster wird eine Liste mit Regeln angezeigt, die von Intego NetBarrier X4 verwendet werden, um Anzeigenbanner zu filtern. Dies ermöglicht es Ihnen, erheblich schneller im World Wide Web zu surfen. Anzeigenbanner sind Anzeigengrafiken, die normalerweise an der Oberseite einer HTML-Seite angezeigt werden. Anzeigenbanner werden von Intego NetBarrier X4 gesperrt und durch transparente Grafiken ersetzt. Durch das Ausfiltern von Anzeigenbannern werden HTML-Seiten erheblich schneller geladen. Ferner werden Sie nicht durch Anzeigen belästigt.

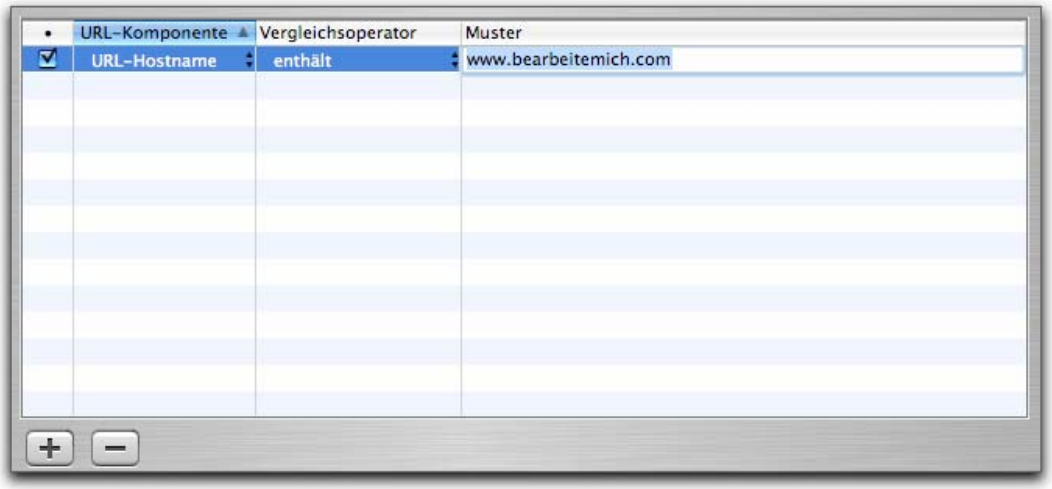


Aktivieren des Datenfilters

Bevor Intego NetBarrier X4 Anzeigenbanner ausfiltern kann, muss der Datenfilter aktiviert sein. Klicken Sie hierzu aufs runde Optionsfeld „Ein“. Sie können den Bannerfilter jederzeit abschalten, wenn Sie vorübergehend Daten von allen Servern akzeptieren wollen, indem Sie aufs runde Optionsfeld „Aus“ klicken.

Definieren von Regeln für den Bannerfilter

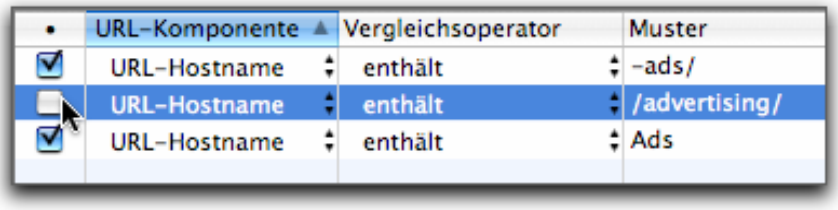
Der Filter enthält bereits eine Reihe von Regeln, die jedes Mal aktualisiert werden, wenn Sie Ihre Filter für NetBarrier X4 mit NetUpdate X4 aktualisieren. Sie können jedoch auch einfach Ihre eigenen Regeln hinzufügen. Klicken Sie hierzu auf die Schaltfläche „+“ in der unteren linken Ecke des Fensterabschnitts. So wird der Banner-Liste eine neue Zeile hinzugefügt, die Sie bearbeiten können.



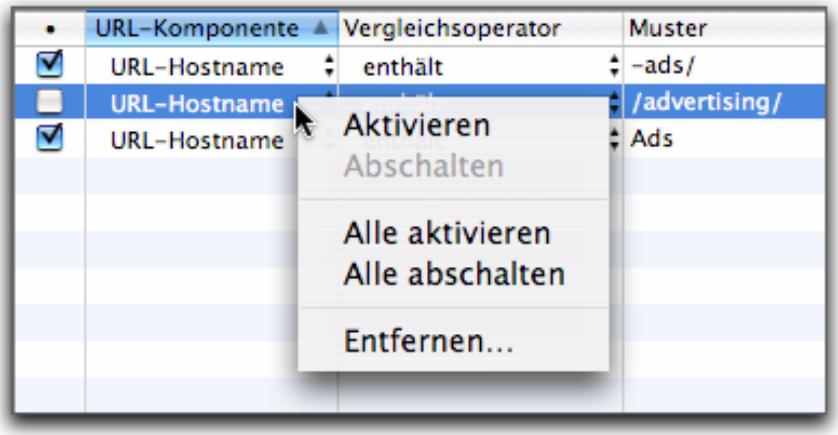
Die Liste besteht aus vier Spalten: ein Kontrollkästchen, URL-Komponente, Vergleichsoperator und Muster. Wenn Sie eine Regel für den Bannerfilter definieren wollen, müssen Sie aus dem Popup-Menü für die URL-Komponente die Option „URL-Hostname“ oder „URL-Pfad“ und dann aus dem Popup-Menü für den Vergleichsoperator die Option „ist“ oder „enthält“ wählen. Geben Sie in das Musterfeld die Textzeichenfolge für den URL ein, den Sie sperren möchten. Wenn Sie beispielsweise Werbebanner vom Server „doubleclick.net“ sperren wollen, müssen Sie die Option „URL-Hostname enthält“ wählen und dann ins Musterfeld die Zeichenfolge „doubleclick.net“ eingeben.

Aktivieren oder Abschalten von Regeln für den Bannerfilter

Jede Bannerregel wird im Bannerfenster in einer eigenen Zeile angezeigt. Mit Hilfe des Kontrollkästchens links von jeder Zeile können Sie den Filter für jede Bannerregel aktivieren oder abschalten. Wenn Sie eine neue Bannerregel hinzufügen, wird das Kontrollkästchen automatisch markiert, wodurch angezeigt wird, dass der Filter für diese Regel aktiviert wurde. Wenn Sie bestimmte Anzeigenbanner nicht mehr sperren lassen wollen, müssen Sie die Markierungen aus den Kontrollkästchen für die betreffenden Banner entfernen.



Sie können auch Banner für eine bestimmte Bannerregel oder für alle Bannerregeln aktivieren. Klicken Sie hierzu bei gedrückter Taste „ctrl“ auf der Tastatur Ihres Macintosh auf den Namen einer Bannerregel. Nun wird ein Kontextmenü geöffnet.



Wählen Sie die Menüoption „Aktivieren“ für die gewünschte Bannerregel oder die Menüoption „Alle aktivieren“, um den Schutz für alle Bannerregeln zu aktivieren.

Auf die gleiche Weise können Sie einzelne oder alle Banneregeln abschalten.

Sie können ein Banner entfernen, indem Sie die Option „Entfernen“ aus dem Kontextmenü wählen oder indem Sie auf die Schaltfläche „-“ in der unteren linken Ecke des Fensterabschnitts für Bannerfilter klicken.

Anmerkung: Beim Verwenden des Bannerfilters kann es vorkommen, dass bestimmte HTML-Seiten nicht mehr korrekt geladen werden. Am besten schalten Sie in diesem Fall den Bannerfilter ab; der URL der HTML-Seite enthält dann höchstwahrscheinlich Text, der Bestandteil der Regel für den Bannerfilter ist.

Cookie-Manager

Ein Cookie ist eine kleine Datei, die von einem Server auf der Festplatte Ihres Computers gespeichert wird. Manche Websites verwenden Cookies, um Informationen über Sie zu sammeln. Cookies können Ihre Benutzerkennung und Ihr Passwort für den Zugriff auf bestimmte Websites, Informationen zur Identifizierung Ihrer Person durch e-Commerce-Server und andere Informationen speichern, auf deren Basis Ihr Surfverhalten analysiert werden kann, ohne dass Sie davon jemals etwas erfahren. Cookies sind nicht grundsätzlich etwas Schlechtes (in den meisten Fällen können Sie ohne Cookies keine Einkäufe im Internet abwickeln), doch manche Websites verwenden sie, um Ihr Surfverhalten zu analysieren.

Intego NetBarrier X4 ermöglicht es Ihnen, exakt festzulegen, was mit Cookies auf Ihrem Computer geschehen soll. Sie können jedes Cookie auf Ihrem Computer prüfen, ändern oder löschen. Ferner können Sie alle Cookies auf Ihrem Computer löschen.

Intego NetBarrier X4 verwaltet die Cookies für die folgenden Anwendungsprogramme: Camino, Firefox, iCab, Internet Explorer, OmniWeb, Opera, Safari, Sherlock, BumpeCar, wDesk, wKids und wKiosk.

Löschen von Cookies für ein spezifisches Anwendungsprogramm

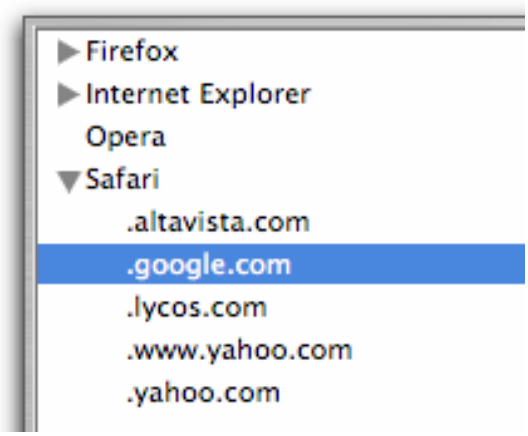
Wenn die Registerkarte „Cookies“ geöffnet ist, sehen Sie eine Liste der Anwendungsprogramme, von denen auf Ihrem Computer Cookies gespeichert wurden. Wenn Sie auf den Namen eines dieser Anwendungsprogramme klicken, werden im rechten Teil des Dialogfelds Informationen über das betreffende Anwendungsprogramm, die Anzahl der von diesem gespeicherten Cookies, die Domänennamen der Server, von denen diese Cookies auf Ihrem Computer gespeichert wurden, und der Zeitpunkt angezeigt, zu dem Sie alle Cookies dieses Anwendungsprogramms zuletzt gelöscht haben.

Wenn Sie alle Cookies für dieses Programm löschen möchten, klicken Sie auf „Alle Cookies löschen…“. Nun wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden,

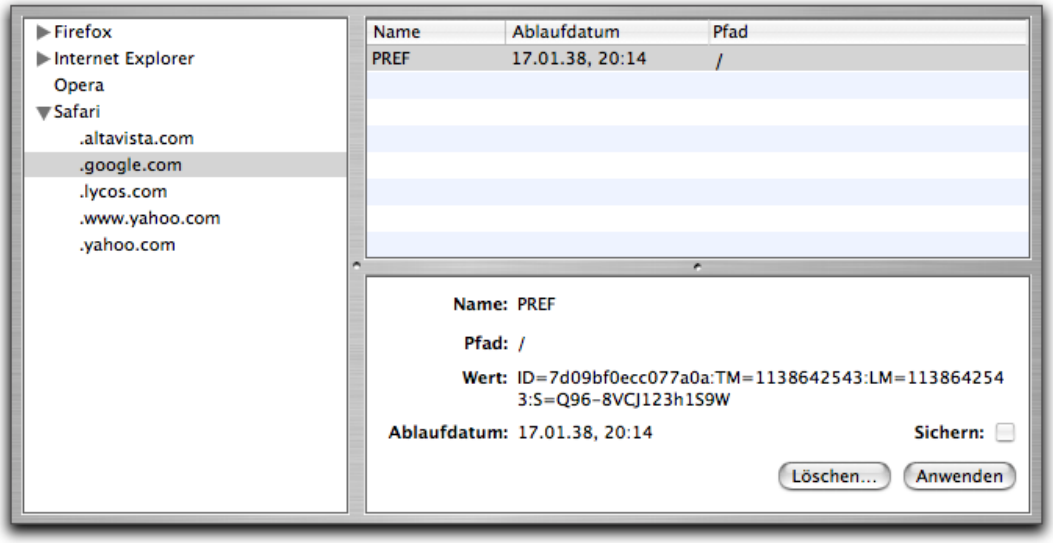
den Löschvorgang zu bestätigen oder abzubrechen. Wenn Sie alle Cookies für ein bestimmtes Anwendungsprogramm löschen, müssen Sie sich bei manchen Websites neu anmelden, wenn diese Cookies verwenden, in denen Ihr Benutzername und Ihr Passwort gespeichert werden.

Ändern einzelner Cookies

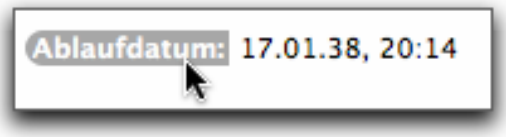
Mit dem Cookie-Manager von Intego NetBarrier X4 können Sie einige Aspekte einzelner Cookies ändern. Um diese Informationen sehen zu können, müssen Sie aufs Schließdreieck links vom jeweiligen Servernamen und dann auf den Namen eines der Cookies von diesem Server klicken.



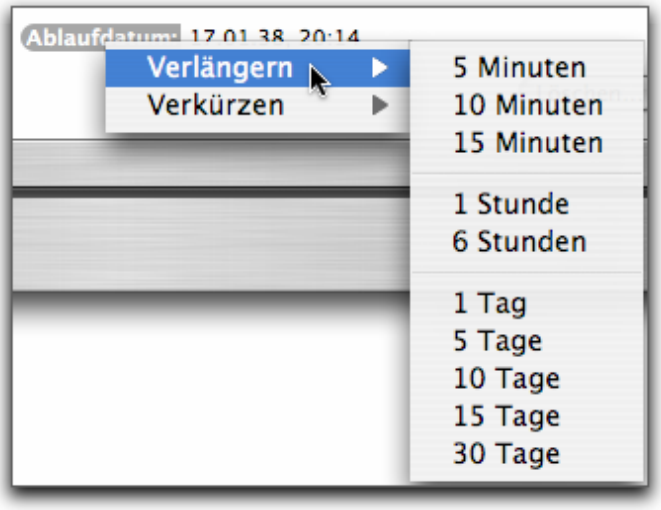
Klicken Sie dann auf einen der Domänennamen in der Liste. Nun wird der Inhalt des Cookies angezeigt.



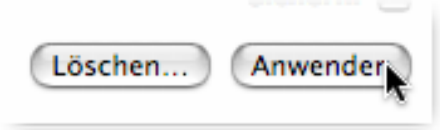
Im obigen Beispiel sehen Sie, dass die in einem Cookie gespeicherten Daten auf irgendeine Weise verschlüsselt sind. Das ist bei Cookies meistens der Fall. Sie können zwar nicht den eigentlichen Inhalt von Cookies, wohl aber ihr Ablaufdatum ändern. Verschieben Sie hierzu den Mauszeiger über das Etikett „Ablaufdatum“, das nun hervorgehoben dargestellt wird.



Klicken Sie auf dieses Etikett und wählen Sie dann die Menüoption „Verlängern“ oder „Verkürzen“. Wählen Sie dann eine Zeit aus dem Popup-Menü.

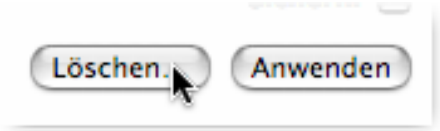


Klicken Sie dann auf die Schaltfläche „Anwenden“, um die Änderungen des Cookies zu bestätigen.



Löschen einzelner Cookies

Sie können nicht nur alle Cookies für ein bestimmtes Anwendungsprogramm, sondern auch einzelne Cookies löschen. Wählen Sie hierzu das gewünschte Cookie und klicken Sie dann auf „Löschen…“.



Nun wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, den Löschvorgang zu bestätigen oder abzubrechen.

Anmerkung: Sie können nur ein Cookie eines inaktiven Anwendungsprogramms löschen. Beenden Sie das Anwendungsprogramm, dessen Cookies Sie löschen wollen. Wenn Sie versuchen ein Cookie zu löschen, während das Programm geöffnet ist, das dieses Cookie verwendet, wird Ihnen eine Mitteilung angezeigt. Darin werden Sie darauf hingewiesen, dass Sie das Programm beenden müssen, um die Cookies zu löschen.

Säubern von Webbrowserdateien

Webbrowser speichern viele Dateien auf Ihrem Computer, und zwar auch nach dem Beendigen des Programms. Zu diesen Dateien gehören die temporären Dateien im Cache des Webbrowsers und die Surfprotokolle (Dateien mit Informationen über die besuchten Websites). Diese Dateien benötigen unter Umständen viel Speicherkapazität auf Ihrer Festplatte. Intego NetBarrier X4 ermöglicht es Ihnen, diese Dateien selektiv für jedes zugehörige Anwendungsprogramm zu löschen.

Wenn Sie auf die Registerkarte „Säubern“ klicken, wird eine Liste der Anwendungsprogramme auf Ihrem Computer angezeigt, die auf Ihrem Computer Cache-Dateien und Surfprotokolle gespeichert haben.

Intego NetBarrier X4 verwaltet die Cache-Dateien für die folgenden Anwendungsprogramme: Camino, Firefox, iCab, Internet Explorer, Opera, Safari, Sherlock, Watson, BumpeCar, wDesk, wKids, wKiosk, Shiira, KidsBrowser und Internet Kiosk. Intego NetBarrier X4 verwaltet die Surfprotokolle für die folgenden Anwendungsprogramme: Firefox, Internet Explorer, Opera, Safari, iCab, BumperCar, Shiira, wKids, wKiosk und wDesk.

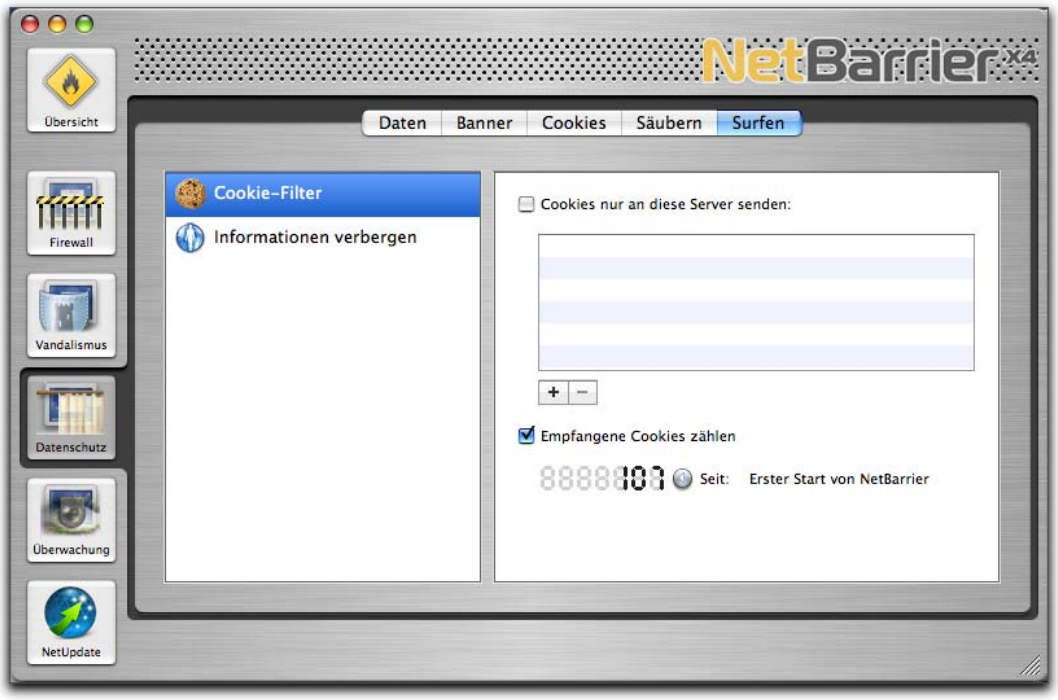
Wenn Sie die Cache-Dateien oder die Surfprotokolle eines Anwendungsprogramms löschen wollen, müssen Sie auf den Namen des betreffenden Anwendungsprogramms in der Programmliste klicken.

Im rechten Teil des Dialogfelds werden der Name und das Symbol des Anwendungsprogramms, die von den Cache-Dateien oder den Surfprotokollen belegte Speicherkapazität auf der Festplatte und der Zeitpunkt des letzten Löschens dieser Dateien angezeigt. Wenn Sie die gewählten Dateien löschen wollen, müssen Sie auf die

Schaltfläche „Säubern…“ klicken. Nun wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, den Löschvorgang zu bestätigen oder abzubrechen.

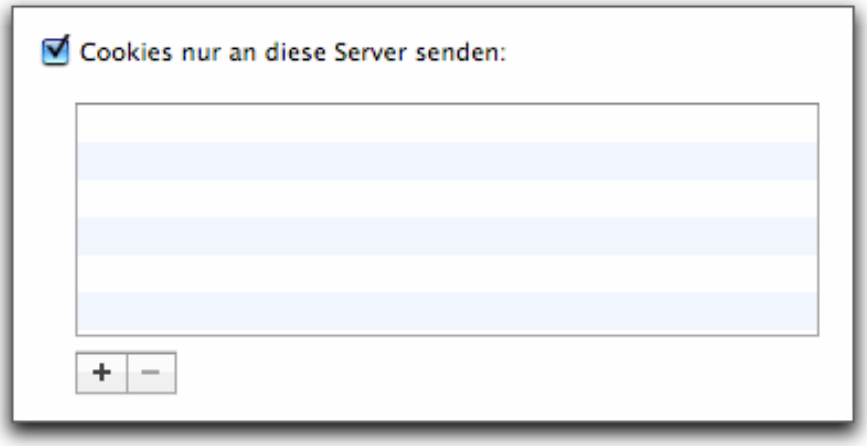
Surffilter

Intego NetBarrier X4 verfügt über weitere Funktionen, mit deren Hilfe Sie Ihre persönlichen Daten schützen können. Auf der Registerkarte „Surfen“ stehen Ihnen spezielle Optionen zur Auswahl zur Verfügung, mit denen Sie festlegen können, wie Cookies und andere Informationen über Ihren Computer behandelt werden sollen.

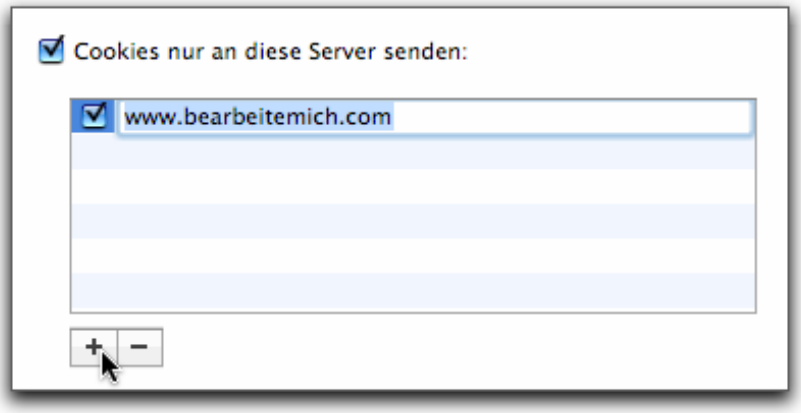


Cookie-Filter

Zusätzlich zu den Funktionen des Cookie-Managers auf der Registerkarte „Cookies“ ermöglicht Ihnen Intego NetBarrier X4, anzugeben, an welche Server Cookies zurückgesandt werden sollen. Wenn Sie das Kontrollkästchen „Cookies nur an diese Server senden“ markiert haben, werden Cookies nur an die freigegebenen Server zurückgesandt. Anmerkung: Wenn das Kontrollkästchen „Cookies nur an diese Server senden“ markiert ist, können Sie unter Umständen nicht mehr auf einige Websites zugreifen, die versuchen, Sie über Cookies zu identifizieren. Dies trifft auf die meisten e-Commerce-Websites zu.



Wenn Sie der Cookie-Filterliste einen Server hinzufügen möchten, klicken Sie auf die Schaltfläche „+“. Daraufhin wird eine Muster-Serveradresse (www.bearbeitemich.com) angezeigt.

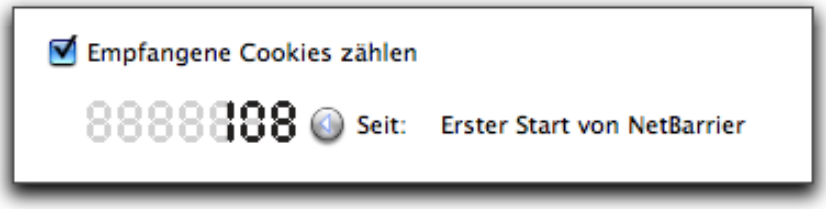


Löschen Sie die Muster-Serveradresse und geben Sie den Namen des Servers ein, dem Sie es gestatten möchten, Ihnen Cookies zuzusenden.

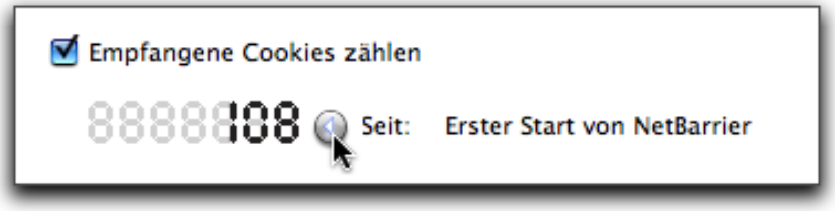
Wenn Sie dieses Kontrollkästchen markieren und das Adressfeld für den Server nicht ausfüllen, sperrt Intego NetBarrier X4 alle Cookie-Anfragen an Ihren Computer.

Cookie-Zähler

Intego NetBarrier X4 kann auch die Anzahl der an Ihren Computer gesendeten Cookies zählen. Hierzu müssen Sie nur das Kontrollkästchen „Empfangene Cookies zählen“ markieren. Nun wird die Anzahl aller seit dem erstmaligen Starten von NetBarrier X4 oder dem Zurücksetzen des Cookie-Zählers empfangenen Cookies angezeigt.



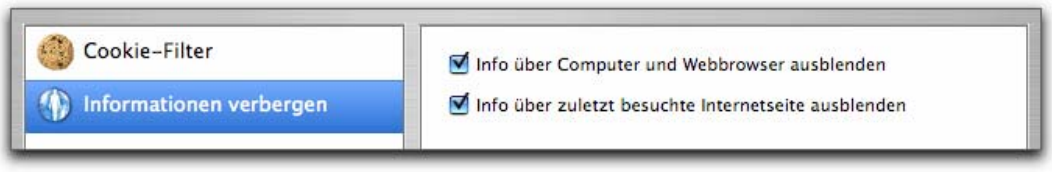
Sie können diesen Zähler durch Klicken aufs Symbol rechts von der Ziffernanzeige zurücksetzen. Hierdurch wird der Cookie-Zähler für *sämtliche* Benutzer Ihres Computers zurückgesetzt.



Nun wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, den Löschvorgang zu bestätigen oder abzubrechen.

Ausblenden der Informationen

Alle Webbrowser reagieren auf Anfragen von Websites, mit denen festgestellt werden soll, welches Betriebssystem (Macintosh, Windows, Linux usw.) und welchen Webbrowser bzw. welche Browserversion Sie verwenden. Dies ist unter Umständen zweckmäßig, wenn Sie eine Website besuchen, deren HTML-Seiten speziell für bestimmte Typen von Webbrowsers optimiert wurden. Diese Funktion ist vor allem zweckmäßig, wenn Sie eine Website besuchen, die versucht, Benutzer mit einem Macintosh-Computer „auszusperren“. Intego NetBarrier X4 kann einige Informationen über Ihren Computer verfälschen.



Intego NetBarrier X4 kann auf diese Abfragen reagieren und nur allgemeine Informationen über Ihren Computer versenden. Beispielsweise kann Intego NetBarrier X4 einem Website-Server mitteilen, dass Sie den Webbrowser Netscape Navigator mit unbekannter Versionsnummer verwenden. Als Betriebssystem kann Intego NetBarrier X4 ebenfalls „unbekannt“ angeben. Wenn Sie wollen, dass Intego NetBarrier X4 die Informationen über Ihren Computer ausblendet, müssen Sie das Kontrollkästchen „Info über Computer und Webbrowser ausblenden“ markieren.

Einige Websites fragen auch ab, welche HTML-Seite Sie zuletzt geladen haben. Dies ist zwar für Betreiber von Websites von Nutzen (da sie nun wissen, von welcher Website Sie auf ihre Website verwiesen wurden), doch skrupellose Website-Betreiber könnten auf diese Weise Ihr Surfverhalten analysieren. Durch Markieren des Kontrollkästchens „Info über zuletzt besuchte Internetseite ausblenden“ wird Intego NetBarrier X4 angewiesen, diese Informationen nicht zu senden.

Überwachung

Im Fenster „Überwachung“ von Intego NetBarrier X4 werden Informationen über die Netzwerkaktivitäten Ihres Computers angezeigt.

Datenverkehr

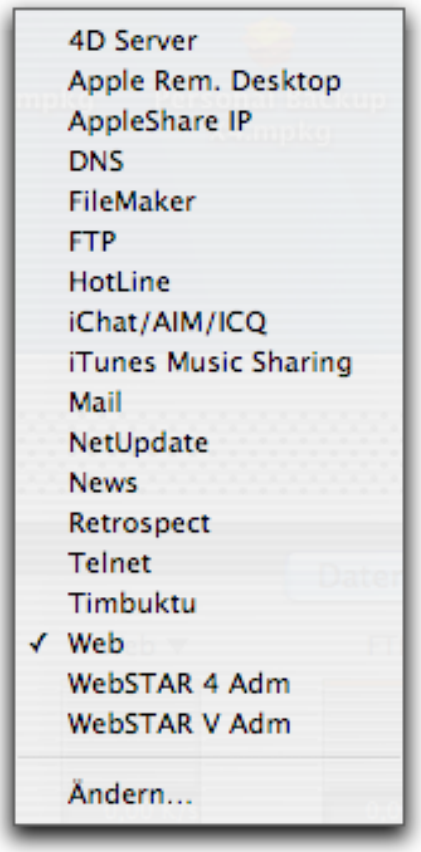
Auf der Registerkarte „Datenverkehr“ befinden sich mehrere Messskalen für die Anzeige der Netzwerkaktivitäten in Verbindung mit ein- und ausgehendem Datenverkehr.

Auf dieser Registerkarte sehen Sie zwei Reihen von Messskalen zur Anzeige der Netzwerkaktivitäten: Die orangefarbenen Messskalen in der oberen Reihe zeigen den eingehenden Datenverkehr und die grünen Messskalen in der Reihe darunter den ausgehenden Datenverkehr an. Die obere Zahl auf jeder Messskala ist der aktuelle Datendurchsatz pro Sekunde und die obere Zahl die gesamte Menge der übertragenen Daten.

Auswählen der Arten von Netzwerkaktivitäten

Sie können wählen, welche Netzwerkaktivitäten von den vier ersten Paaren von Messskalen angezeigt werden sollen. Klicken Sie hierzu aufs Popup-Menü über der betreffenden Messskala zur Anzeige der Netzwerkaktivitäten.

Nun können Sie den Typ der Netzwerkaktivitäten auswählen.



Folgende Arten von Netzwerkaktivitäten können aufgezeichnet werden:

4D Server:	Daten von 4D Server.
Apple Rem. Desktop:	Daten von Apple Remote Desktop.
AppleShare IP:	Daten von AppleShare IP.
DNS:	DNS-Daten.
FileMaker:	Daten von FileMaker Pro.
FTP:	FTP-Daten.
Hotline:	Daten von oder zu einem Hotline-Server.
iChat/AIM/ICQ:	Daten von iChat, AIM oder ICQ.

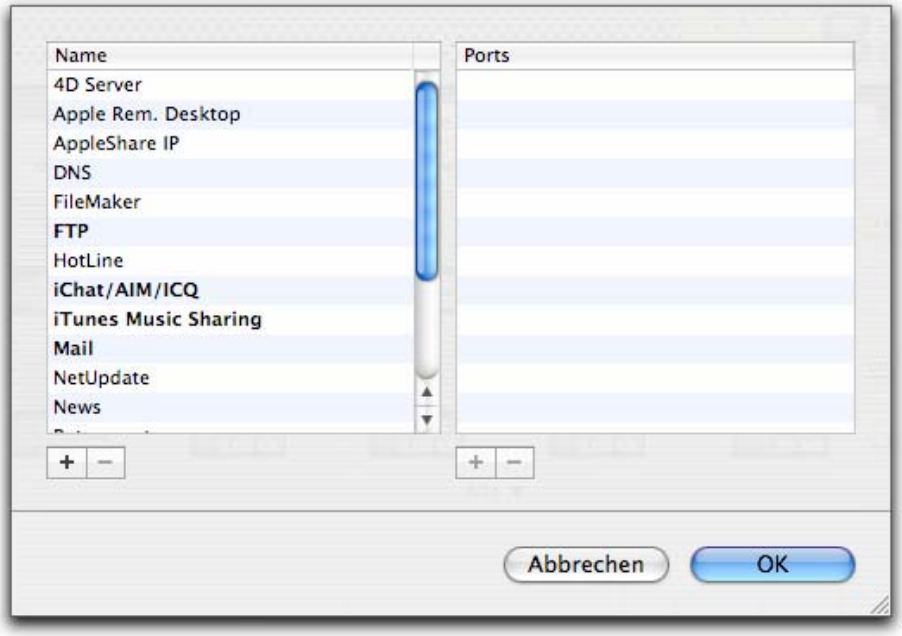
iTunes Music Sharing:	Daten für die gemeinsame Verwendung von iTunes Music.
E-Mail:	E-Mail-Daten.
NetUpdate:	Daten, die von Intego NetUpdate empfangen oder gesendet werden.
News:	Newsgroup-Daten.
Retrospect:	Daten von Retrospect.
Telnet:	Telnet-Daten.
Timbuktu:	Daten von Timbuktu.
Web:	Daten von oder zu Website-Servern (HTTP).
WebSTAR 4 Adm:	WebSTAR-Verwaltungsdaten.
WebSTAR V Adm:	WebSTAR-Verwaltungsdaten.
Ändern:	Erlaubt Ihnen das Verändern, Hinzufügen oder Löschen von Datentypen (siehe unten).

Für die beiden letzten Messskalen kann die Art der Netzwerkaktivitäten nicht gewählt werden. Diese Messskalen zeigen folgende Informationen an:

Sonstige:	Die Daten für andere Protokolle.
IP:	Die Gesamtmenge aller IP-Daten – die Summe der ersten drei Messskalen.

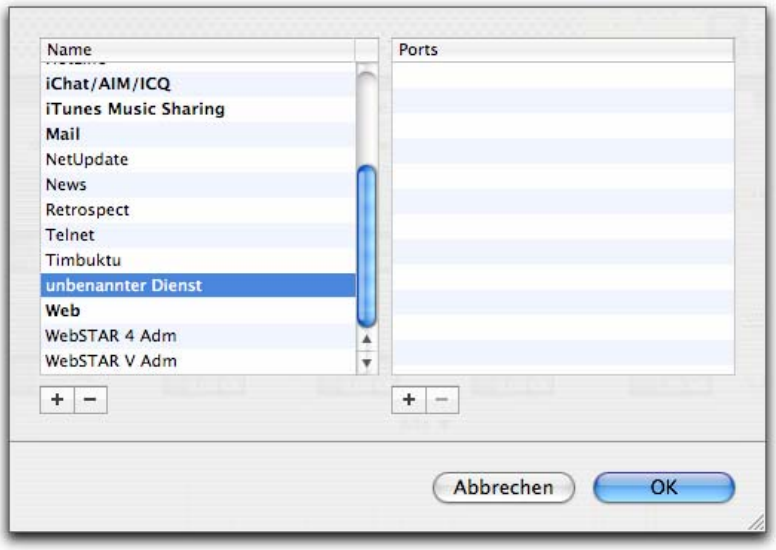
Hinzufügen von Diensten zu den Messskalen zur Anzeige der Netzwerkaktivitäten

Sie können der Liste Ihre eigenen Dienste hinzufügen, indem Sie „Ändern…“ aus der Liste der Aktivitätsdatentypen wählen. Hierauf wird eine Liste der Dienste angezeigt.



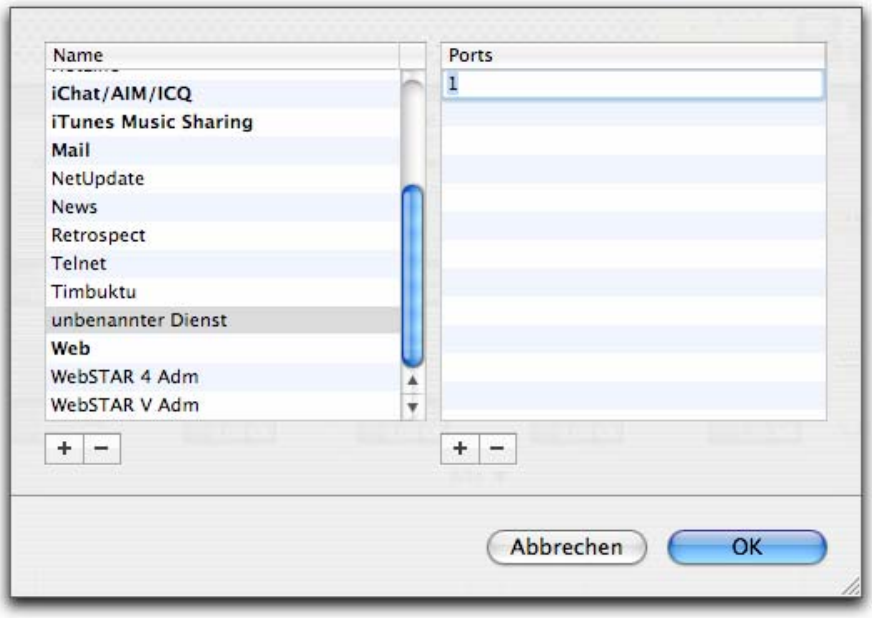
In dieser Liste sind alle Dienste aufgeführt, deren Netzwerkaktivitäten von den Messskalen erfasst werden. Sie können einen Dienst aus der Spalte „Name“ wählen und auf die Schaltfläche „OK“ klicken, um ihn zum Menü „Aktivitätsdatentyp“ hinzuzufügen.

Sie können auch Ihre eigenen Dienste definieren und diese in die Liste der aktivierten Dienste aufnehmen. Klicken Sie auf die Schaltfläche „+“ unter der Spalte „Name“, wenn Sie einen neuen Dienst hinzufügen möchten. Die Liste der aktivierten Dienste wird nun um eine Zeile erweitert.



Geben Sie einen Namen für den neuen Dienst ein und drücken Sie die Rücklauftaste.

Damit die Netzwerkaktivität für diesen Dienst erfasst werden kann, müssen Sie angeben, welche Ports von diesem Dienst verwendet werden. Klicken Sie hierzu auf die Schaltfläche „+“ unter der Spalte „Ports“.



An der Oberseite der Port-Liste erscheint eine neue Zeile. Geben Sie die Port-Nummer oder eine Reihe von Port-Nummern (beispielsweise 110-123) für Ihren neuen Dienst ein und drücken Sie anschließend auf die Eingabetaste. Auf diese Weise können Sie auch mehrere Ports hinzufügen. Sie können einen Port aus der Port-Liste löschen, indem Sie auf seine Nummer und dann auf die Schaltfläche „-“ klicken.

Sie können Dienste auch per Drag&Drop aus der Dienste-Bibliothek hinzufügen. Dies ist besonders dann hilfreich, wenn Sie die entsprechenden Port-Nummern nicht kennen, die Sie der Liste hinzufügen möchten. Gehen Sie zum Öffnen der Dienste-Bibliothek in den Abschnitt „Firewall“. Klicken Sie auf den Reiter „Allgemeines“ und anschließend auf die Schaltfläche „Dienste-Bibliothek“ in der unteren rechten Ecke. Wählen Sie den gewünschten Dienst aus und ziehen Sie ihn in die Port-Liste.

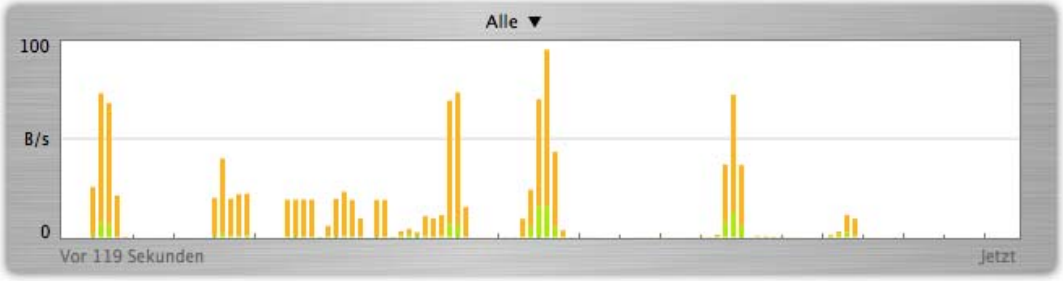
Klicken Sie auf „OK“. So wird der neue Dienst in der Liste gespeichert.

Ändern von Diensten

Sie können die Ports ändern, die den verschiedenen Diensten zugewiesen sind. Klicken Sie hierzu auf den Namen des betreffenden Dienstes. Nun können Sie die zugehörigen Ports im rechten Teil des Fensters hinzufügen, löschen oder ändern. Klicken Sie nun auf die Schaltfläche „OK“, um die Änderungen zu speichern, oder auf die Schaltfläche „Abbrechen“, um die Änderungen nicht wirksam werden zu lassen.

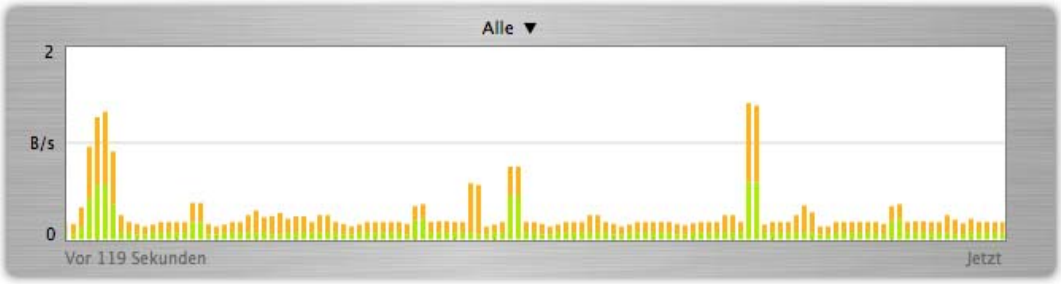
Diagramm mit dem gesamten Datenverkehrsaufkommen

In diesem Fenster wird ein Balkendiagramm des gesamten Datenverkehrsaufkommens angezeigt. Wenn keine Netzwerkaktivitäten stattfinden, wird in diesem Fenster nichts angezeigt. Bei Netzwerkaktivitäten über ein lokales Netzwerk oder das Internet werden in diesem Fenster die gesamten Netzwerkaktivitäten angezeigt.



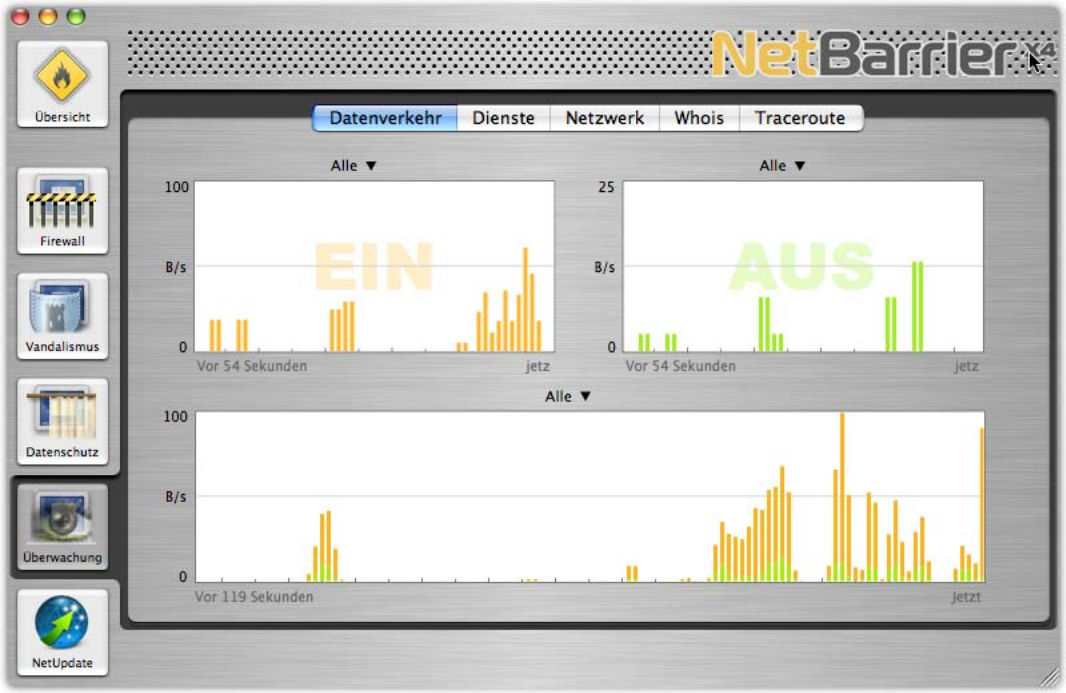
Der eingehende Datenverkehr wird orangefarben und der ausgehende Datenverkehr grün angezeigt.

Dieses Diagramm wird dynamisch skaliert: es ändert sich in Abhängigkeit vom Datenverkehrsaufkommen. Im vorstehenden Beispiel ist eine Netzwerkverbindung aktiv; der Datendurchsatz beträgt ca. 0 bis 98 KByte/s. Im zweiten Beispiel darunter werden die meisten Daten über ein lokales Netzwerk abgerufen; hier liegt der maximale Datendurchsatz bei 1,5 Kilobytes pro Sekunde.



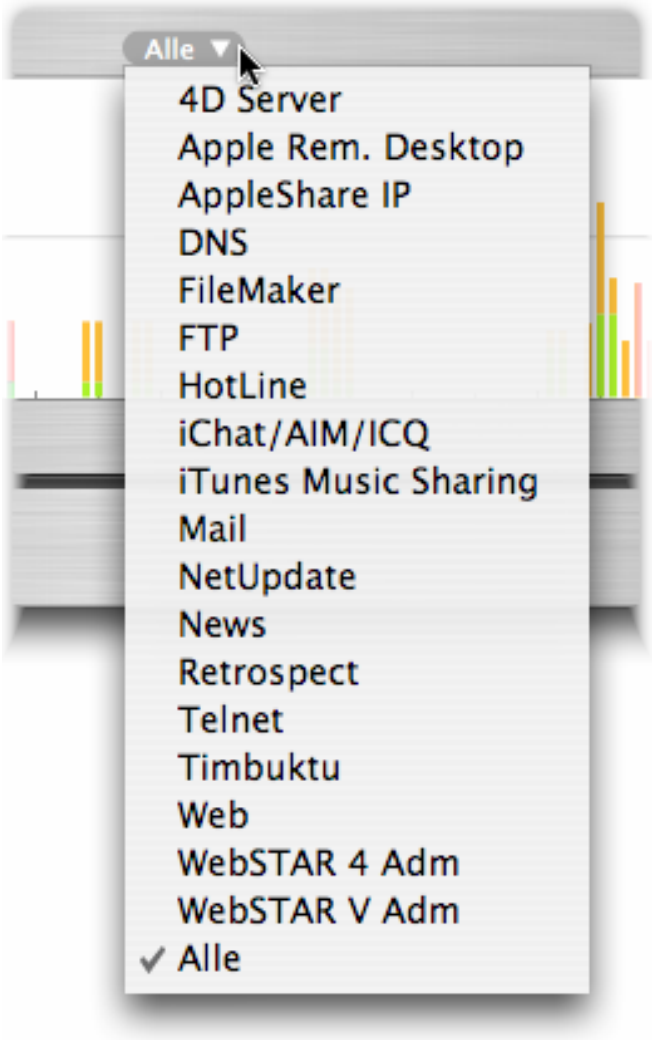
Wenn Sie den Mauszeiger über dieses Diagramm verschieben, wird ein Text angezeigt, aus dem der aktuelle Datendurchsatz ersichtlich ist. Der Wert des Datendurchsatzes wird einmal pro Sekunde aktualisiert.

Wenn Sie separate Diagramme für ein- und ausgehenden Datenverkehr sehen wollen, müssen Sie nur an beliebiger Stelle ins Diagramm doppelklicken. Im Diagrammfenster sehen Sie nun drei Diagramme: eines für eingehenden Datenverkehr, eines für ausgehenden Datenverkehr und eines für den gesamten Datenverkehr.

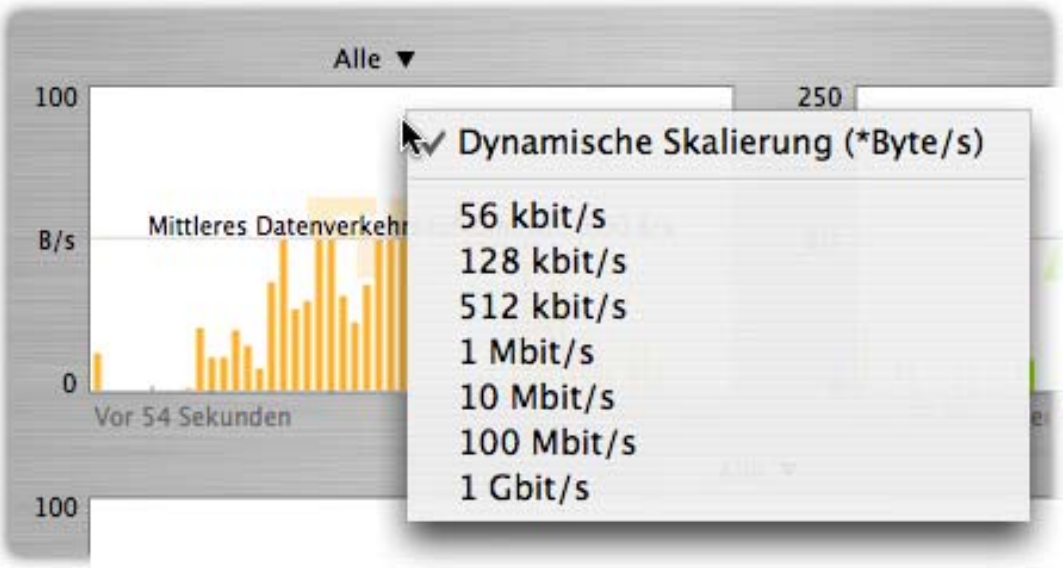


Wenn Sie wieder die Normalansicht mit einem einzelnen Diagramm und nur einem Satz von Messskalen zur Anzeige der Netzwerkaktivitäten aufrufen wollen, müssen Sie nur noch einmal an beliebiger Stelle in eines der Diagramme doppelklicken.

Sie können auch den in den Diagrammen angezeigten Datentyp ändern. Klicken Sie hierzu auf die Schaltfläche „Alle“ direkt über dem Diagramm und wählen Sie dann einen Datentyp aus dem Popup-Menü.



Wenn im Fenster drei Diagramme angezeigt werden, können Sie die Skalierung für die Diagramme für ein- und ausgehenden Datenverkehr wählen. Wenn Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh auf eine beliebige Stelle des Diagramms für ein- oder ausgehenden Datenverkehr klicken, wird ein Popup-Menü mit mehreren Optionen geöffnet.



Damit können Sie die korrekte Skalierung der Diagramme für die Anzeige der zu erwartenden Datendurchsätze wählen. Wählen Sie die Option „Dynamische Skalierung“, wenn sich die Skalierung der Diagramme automatisch in Abhängigkeit vom Datendurchsatz ändern soll.

Zurücksetzen der Messskalen zur Anzeige der Netzwerkaktivitäten

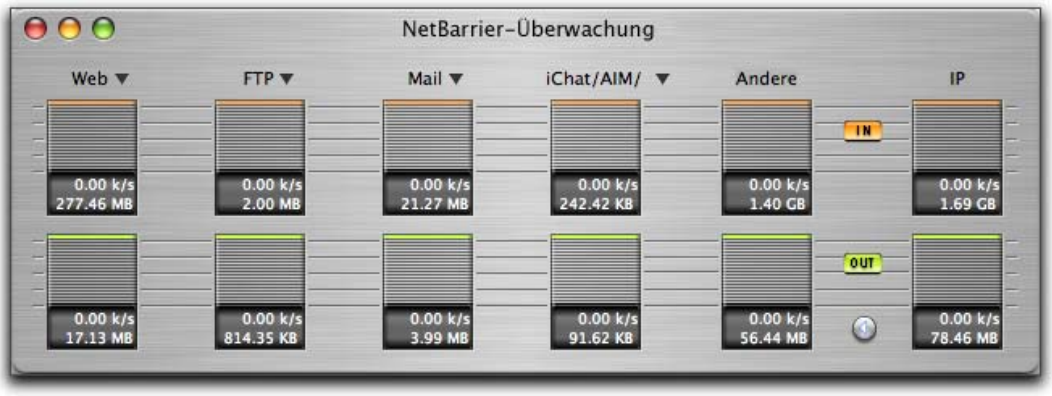
Sie können die Gesamtanzeigewerte der Messskalen zur Anzeige der Netzwerkaktivitäten zurücksetzen (auf Null setzen), indem Sie auf die Schaltfläche mit dem nach links weisenden Dreieck klicken.

Nach dem Klicken auf diese Schaltfläche wird eine Warnmeldung ausgegeben, in der Sie aufgefordert werden, das Zurücksetzen der Messskalen zur Anzeige der Netzwerkaktivitäten zu bestätigen. Hierdurch wird sichergestellt, dass Sie die Messskalen zur Anzeige der Netzwerkaktivitäten nicht versehentlich zurücksetzen. Wenn Sie die Messskalen zurücksetzen wollen, müssen Sie auf die Schaltfläche „Zurücksetzen“ klicken. Klicken Sie andernfalls auf die Schaltfläche „Abbrechen“.

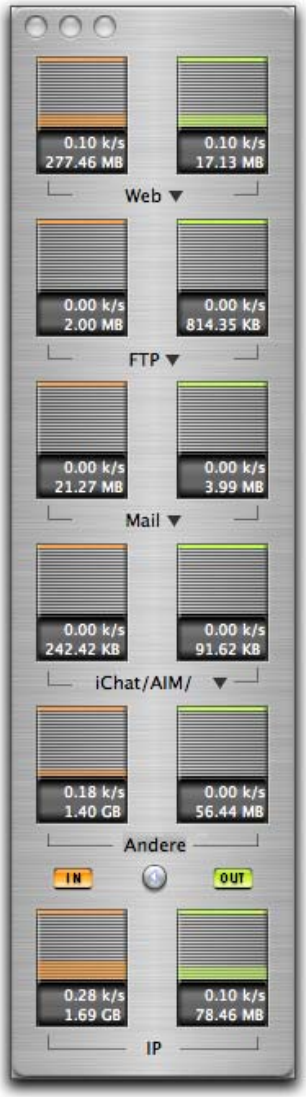
Anzeigen der Messskalen zur Anzeige der Netzwerkaktivitäten als Palette

Wenn Sie auf die Schaltfläche zur Veränderung der Fenstergröße klicken,

wird das Fenster von Intego NetBarrier X4 minimiert und die Messskalen zur Anzeige der Netzwerkaktivität werden als horizontale Palette eingeblendet.

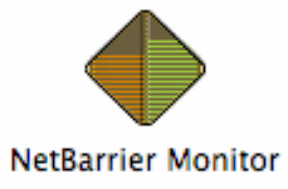


Wenn Sie bei gedrückter Umschalttaste auf die Schaltfläche zur Veränderung der Fenstergröße klicken, wird die Palette vertikal ausgerichtet. Dies ist unter Umständen zweckmäßig, wenn Sie die Netzwerkaktivitäten während der Arbeit an Ihrem Computer ständig überwachen wollen. Wenn Sie wieder das Hauptfenster von Intego NetBarrier X4 sehen wollen, müssen Sie nur aufs Schließfeld der horizontal oder vertikal ausgerichteten Palette klicken.



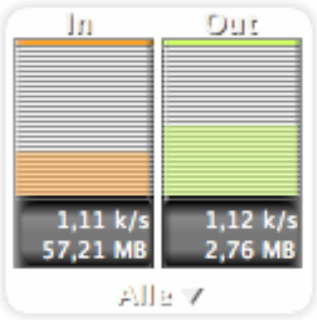
Verwenden des Programms NetBarrier-Monitor

Gleichzeitig mit Intego NetBarrier X4 wird auch das Programm NetBarrier-Monitor installiert. Dieses Dienstprogramm finden Sie im Ordner „Programme“.



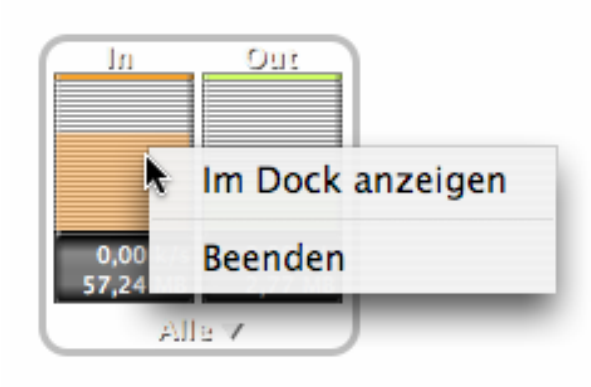
NetBarrier-Monitor öffnet ein kleines, schwebendes Fenster, das es Ihnen ermöglicht, die Netzwerkaktivitäten ständig zu überwachen, ohne die Palette mit den Messskalen zur Anzeige der Netzwerkaktivitäten geöffnet halten zu müssen.

Nach dem Starten von NetBarrier-Monitor wird dessen Fenster mit den Messskalen in der unteren rechten Bildschirmecke angezeigt.



Standardmäßig zeigt NetBarrier-Monitor den gesamten Datenverkehr für alle Dienste an. Sie können dies ändern, indem Sie auf „Alle“ unten im Fenster klicken und aus dem Popup-Menü einen Dienst wählen.

Wenn Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh auf eine beliebige Stelle des Fensters von NetBarrier-Monitor klicken, wird ein Popup-Menü mit zwei Optionen geöffnet.



Sie können NetBarrier-Monitor beenden, indem Sie die Menüoption „Beenden“ wählen.

Sie können auch festlegen, dass die Messskalen zur Anzeige der Netzwerkaktivitäten von NetBarrier-Monitor im Dock angezeigt werden. Hierzu müssen Sie nur die Menüoption „Im Dock anzeigen“ wählen. Hierauf wird das Fenster von NetBarrier-Monitor geschlossen. Das Symbol von NetBarrier-Monitor im Dock ändert sich, um anzuzeigen, dass die Anzeigen der Messskalen in Echtzeit aktualisiert werden.

Wenn wieder das Fenster von NetBarrier-Monitor geöffnet werden soll, müssen Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh aufs Symbol von NetBarrier-Monitor im Dock klicken und dann die Menüoption „Im Fenster anzeigen“ wählen.

Wenn NetBarrier-Monitor im Dock angezeigt wird, können Sie seine Anzeige ändern, wenn Sie bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh aufs Symbol von NetBarrier-Monitor im Dock klicken und aus dem Dock-Menü einen anderen Dienst wählen.

Aus diesem Menü können Sie auch die Option „Im Dock behalten“ wählen. Dadurch wird das Symbol von NetBarrier-Monitor auch dann im Dock angezeigt, wenn das

Programm nicht läuft, sodass Sie es durch einfaches Klicken auf dieses Symbol starten können.

Voreinstellungen für NetBarrier-Monitor

Für NetBarrier-Monitor stehen zwei Voreinstellungen zur Verfügung. Gehen Sie zum Einrichten der Voreinstellungen in „NetBarrier Monitor“ > „Voreinstellungen“.

- **Über den anderen Fenstern anzeigen**
  Wenn Sie diese Option wählen, werden die Messskalen von NetBarrier-Monitor immer im Vordergrund, über allen anderen Fenstern, angezeigt.

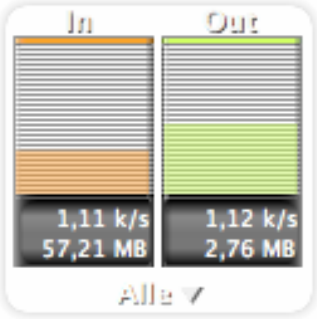
- **Für Mausklicks erkennbar machen**
  Wenn Sie diese Option wählen, werden die Messskalen von NetBarrier-Monitor so angezeigt, dass sie für Mausklicks transparent oder unsichtbar sind. Sie können das Fenster mit den Messskalen dann nicht verschieben oder die Dienste ändern, die Sie gerade überwachen.

Das Widget für NetBarrier-Monitor

Mit Intego NetBarrier X4 wird ein Widget für NetBarrier-Monitor installiert, das in das Dashboard von Mac OS X (nur bei Mac OS X 10.4 Tiger oder neuer) geladen wird. In diesem Widget wird Ihnen jederzeit die Netzwerkaktivität angezeigt.

Wenn Sie sich das Widget für NetBarrier-Monitor anzeigen lassen möchten, öffnen Sie das Dashboard von Mac OS X. Klicken Sie auf die Schaltfläche „+“, wenn Sie sich alle auf Ihrem Computer verfügbaren Widgets anzeigen lassen möchten. Wählen Sie NetBarrier-Monitor aus der Liste. Das Symbol sieht folgendermaßen aus:

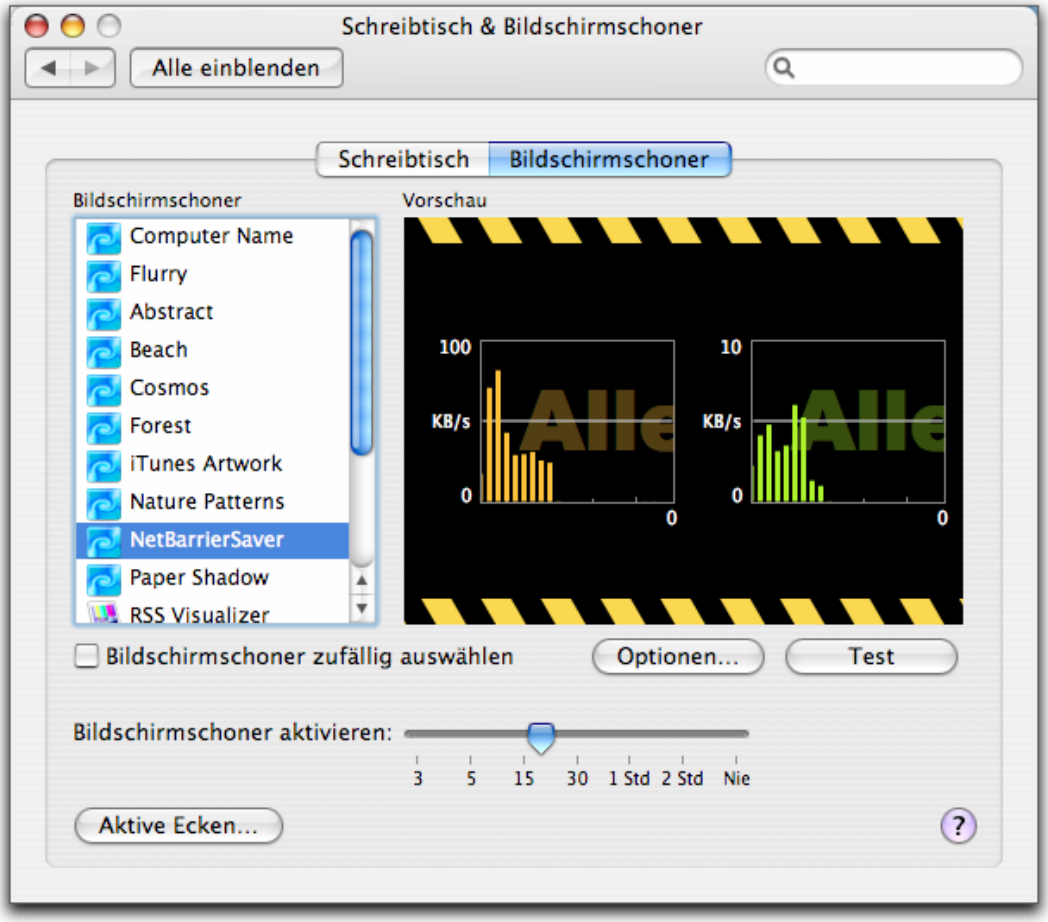
Sobald Sie auf das Symbol klicken, wird es Ihren aktiven Widgets hinzugefügt und zeigt Ihnen dann das folgende Messskalen-Paar an. Sie können die Art der angezeigten Aktivität mit der unter den Messskalen zur Verfügung stehenden Liste ändern. Weitere Informationen erhalten Sie in **Kapitel 5, Verwenden des Programms NetBarrier-Monitor**.



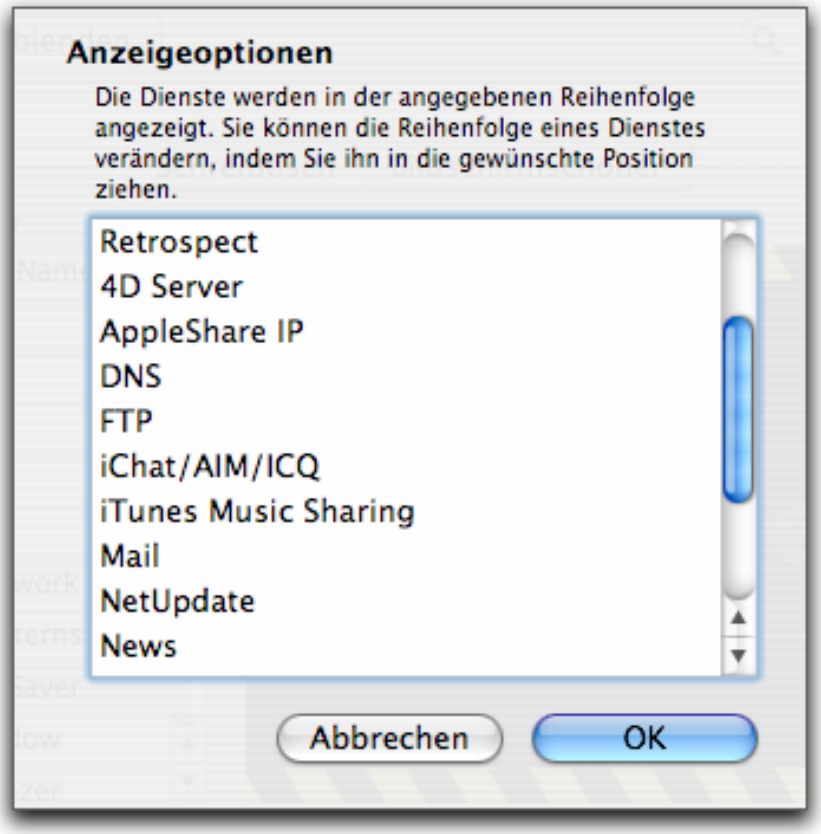
Der Bildschirmschoner von Intego NetBarrier X4

Mit Intego NetBarrier X4 wird auch ein spezieller Bildschirmschoner installiert. Dieser Bildschirmschoner ermöglicht Ihnen einen Überblick über die Netzwerkaktivitäten. Auch wenn Sie gerade nicht arbeiten, können Sie sehen, welche Daten von Ihrem Computer gesendet und empfangen werden. Wenn Ihr Computer als Server betrieben wird, sind Sie stets über die aktuellen Netzwerkaktivitäten informiert.

Wenn Sie den Bildschirmschoner von Intego NetBarrier X4 verwenden wollen, müssen Sie die Menüoption „Systemeinstellungen…“ aus dem Apple-Menü wählen und dann erst auf die Schaltfläche „Schreibtisch & Bildschirmschoner“ und dann auf „Bildschirmschoner“ klicken. Wählen Sie „NetBarrierSaver“ aus der Liste der Bildschirmschoner.



Klicken Sie auf die Schaltfläche „Optionen…“, um den Bildschirmschoner zu konfigurieren. Sie können festlegen, in welcher Reihenfolge die Dienste angezeigt werden sollen.



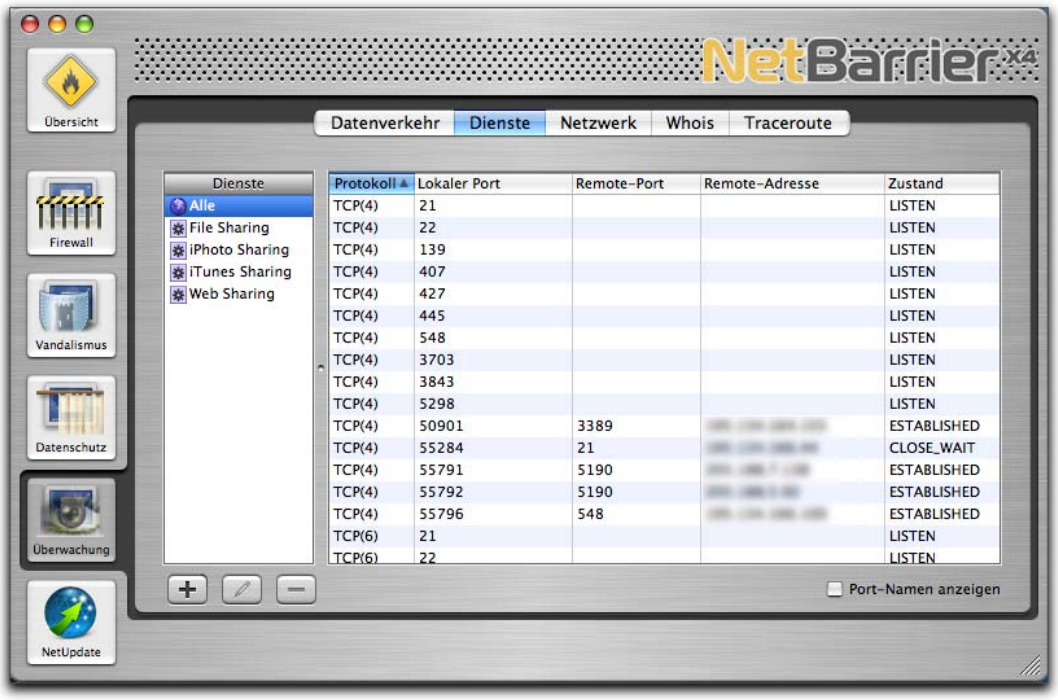
Ziehen Sie die Dienste einfach in die gewünschte Reihenfolge.

Die Anzahl der darstellbaren Dienste hängt von der Größe Ihres Bildschirms, der verwendeten Auflösung (Anzahl der Bildpunkte in beiden Achsen) und der Anzahl der verwendeten Videomonitore ab.

Weitere Informationen über die Einstellung von Bildschirmschonern finden Sie in der Hilfe zu Mac OS X.

Dienste

In diesem Abschnitt werden alle momentan auf Ihrem Computer laufenden Dienste aufgelistet, die anderen Benutzern übers IP-Protokoll zur Verfügung stehen: Webserver, Mailserver usw. Für jeden belegten Port werden die folgenden Informationen angezeigt: Das Protokoll (TCP oder UDP), die Nummer des lokalen Ports, die Nummer des Ports des anderen Computers gemäß dem verwendeten Protokoll, ob es sich um ein Standardprotokoll wie z.B. HTTP auf Port 80 handelt, die IP-Adresse des anderen Computers und der Status der Verbindung. Wenn Sie zusätzlich zu den Port-Nummern auch die Namen der Ports sehen möchten, klicken Sie auf das Kontrollkästchen „Port-Namen anzeigen“ in der unteren rechten Ecke.



Da die Liste der Ports, die von allen Diensten verwendet werden, sehr lang sein kann, bietet NetBarrier X4 Filter an, mit denen Sie sich die Ports anzeigen lassen können, die von bestimmten Diensten verwendet werden. Sie können zwischen File Sharing, iPhoto

Sharing, iTunes Sharing und Web Sharing auswählen. Sie können aber auch eigene Filter erstellen.

Klicken Sie hierzu auf die Schaltfläche „+“ in der unteren linken Ecke des Fensters. Hierauf wird das Dialogfeld „Intelligenter Filter“ geöffnet. Entscheiden Sie zuerst, ob der neue Filter mit allen Bedingungen übereinstimmen soll, die Sie im Anschluss festlegen.

Wählen Sie dann aus dem Popup-Menü die Art der Informationen, auf die der Filter angewendet werden soll. Geben Sie anschließend die entsprechenden Informationen an.

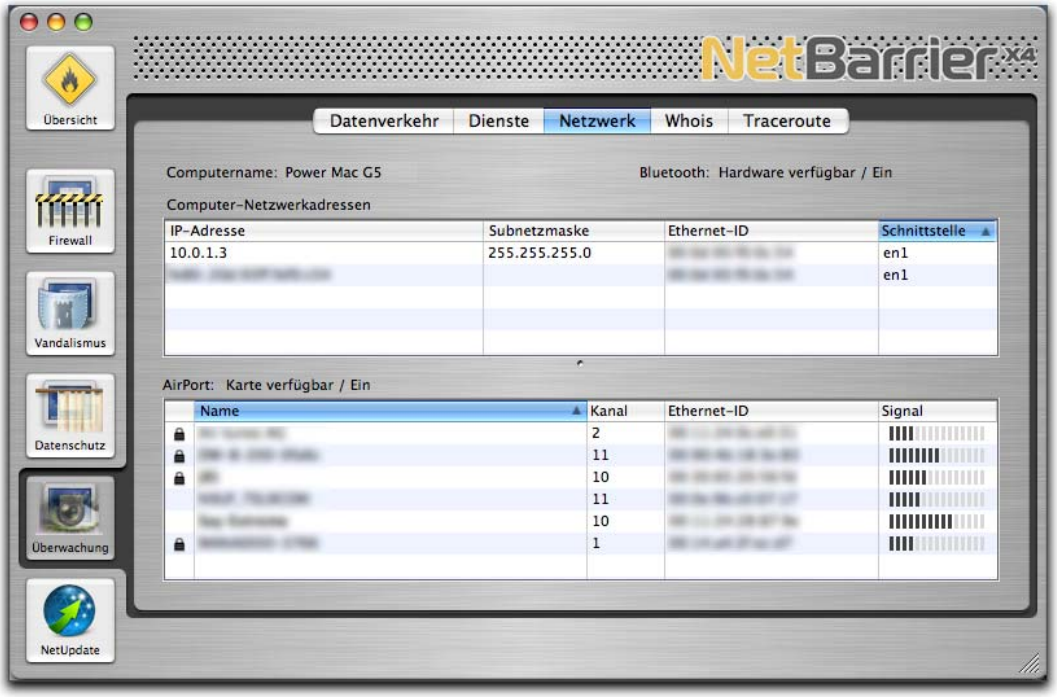
Wenn Sie dem Filter weitere Bedingungen hinzufügen möchten, klicken Sie auf die Schaltfläche „+“ rechts im Fenster. Umgekehrt können Sie auch Bedingungen entfernen, indem Sie auf die Schaltfläche „-“ neben der Bedingung klicken, die entfernt werden soll. Zudem können Sie Filterbedingungen auch verändern, indem Sie einfach die

Option aus dem Popup-Menü ändern oder indem Sie neue Daten in das Datenfeld eingeben.

Wenn Sie die Erstellung des Filters abgeschlossen haben, klicken Sie auf „OK“, um den Filter zu speichern. Sie müssen dann einen Namen für den Filter in der Diensteliste eingeben. Wenn der unbenannte Filter noch nicht ausgewählt wurde, doppelklicken Sie darauf und geben Sie den neuen Namen ein.

Netzwerk

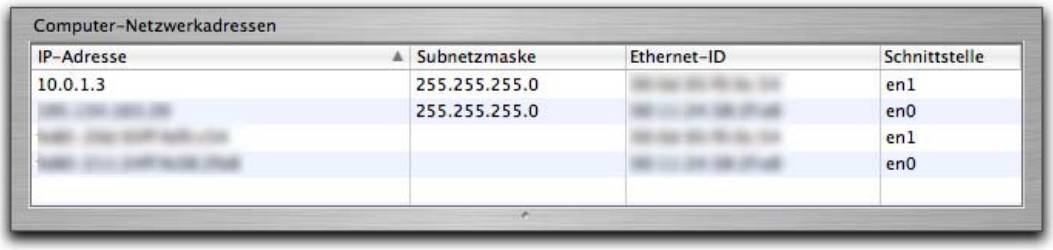
Auf dieser Registerkarte werden nützliche Informationen über Ihren Computer und seine Netzwerkkonfiguration angezeigt.



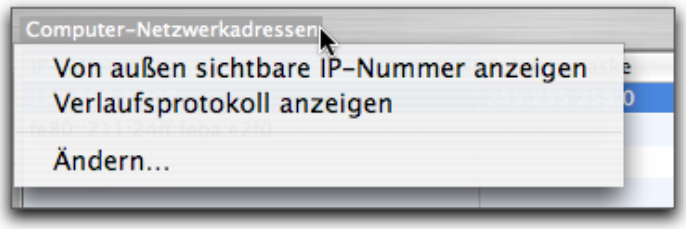
Auf der Registerkarte sehen Sie den Namen des Computers, seine IP-Adresse, ob Bluetooth-Hardware zur Verfügung steht und ob diese aktiviert wurde. Sie können die Sortierungsreihenfolge der Liste ändern, indem Sie auf die Spaltenüberschriften klicken.

Wenn Sie auf „Computername“ klicken, können Sie den Namen Ihres Computers ändern. Wenn Sie auf „Ändern…“ klicken, wird der Fensterabschnitt „Sharing“ in den Systemeinstellungen geöffnet, in dem Sie den Namen Ihres Computers ändern können.

Im Abschnitt „Computer-Netzwerkadressen“ können Sie alle IP-Adressen sehen, die auf Ihrem Computer aktiviert sind. Diese Möglichkeit können Sie nutzen, wenn Sie in Ihrem Computer mehrere Netzwerkkarten mit unterschiedlichen IP-Nummern installiert haben oder mehrere Server betreiben. Das Fenster zeigt Ihnen ebenfalls die Subnetzmaske, die Ethernet-ID und die Schnittstelle der jeweiligen IP-Adresse an.

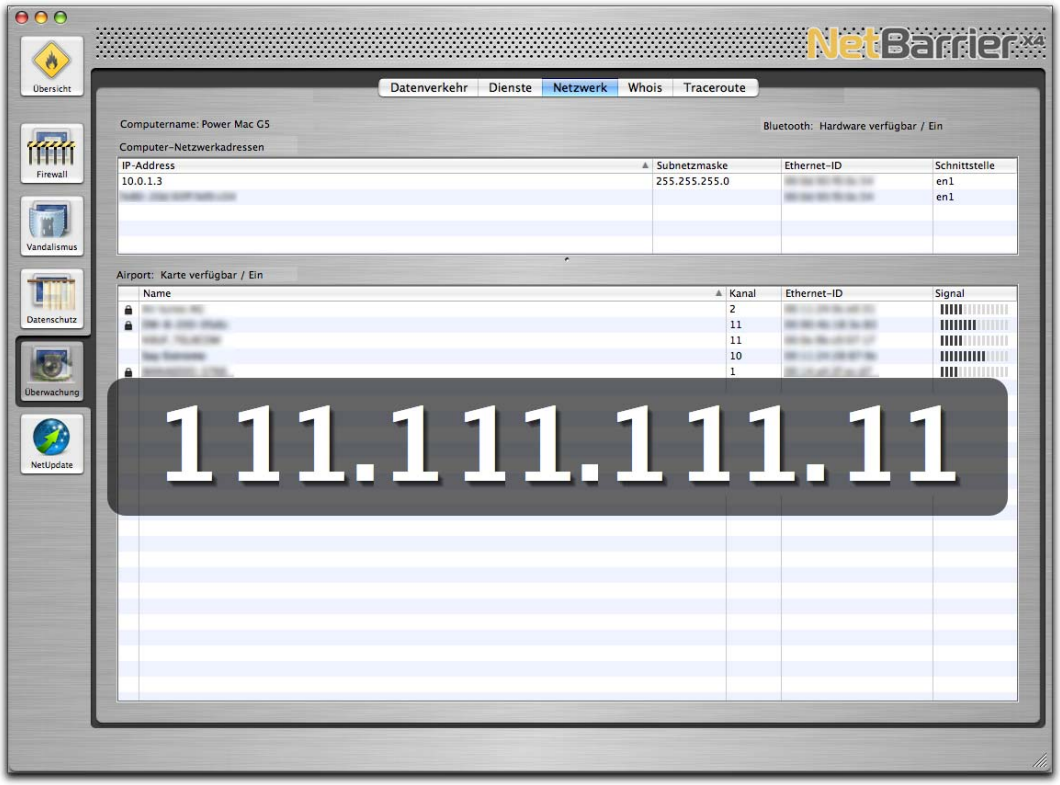


Wenn Sie auf „Computer-Netzwerkadressen“ klicken, wird der Text hervorgehoben und in einem Popup-Menü erscheinen drei Optionen:



Von außen sichtbare IP-Nummer anzeigen

Diese Option zeigt in großer Schrift die von außen sichtbare IP-Adresse an, die Ihr Computer verwendet, wenn er mit dem Internet oder anderen Netzwerken verbunden wird. Diese IP-Nummer unterscheidet sich von der auf dieser Registerkarte angezeigten IP-Nummer, wenn Ihr Computer über einen Router oder einen Kabel- bzw. DSL-Modem mit dem Internet verbunden ist.



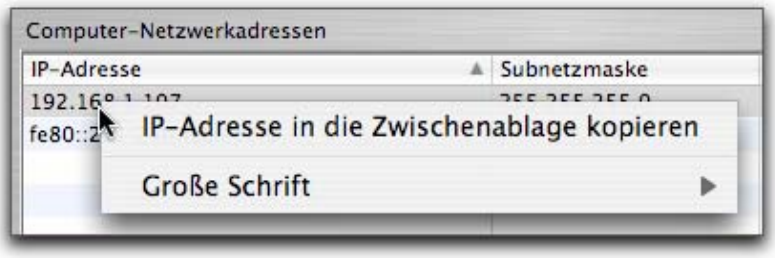
Verlaufsprotokoll anzeigen

Mit Hilfe dieser Option können Sie sich anzeigen lassen, welche IP-Adressen Ihr Computer in der Vergangenheit hatte. Sie sehen eine Liste mit den IP-Adressen, die Ihrem Computer in der Vergangenheit von Ihrem ISP zugewiesen wurden. Dies ist jedoch nur zutreffend, wenn Ihrem Computer keine feste IP-Nummer zugewiesen wurde. Wenn Ihr Computer über einen Router, einen Kabelmodem oder einen DSL-Modem mit dem Internet verbunden ist, wird lediglich die interne IP-Adresse Ihres Computers angezeigt.

Ändern

Wenn Sie auf „Ändern…“ klicken, wird der Fensterabschnitt „Netzwerk“ in den Systemeinstellungen geöffnet. Sie können in diesem Fensterabschnitt die Netzwerkadresse Ihres Computers ändern. Weitere Informationen über die Netzwerkeinstellungen erhalten Sie in der Hilfe zu Mac OS X.

Wenn Sie das Etikett „IP-Adresse“ klicken, wird ein Popup-Menü mit weiteren Optionen geöffnet.



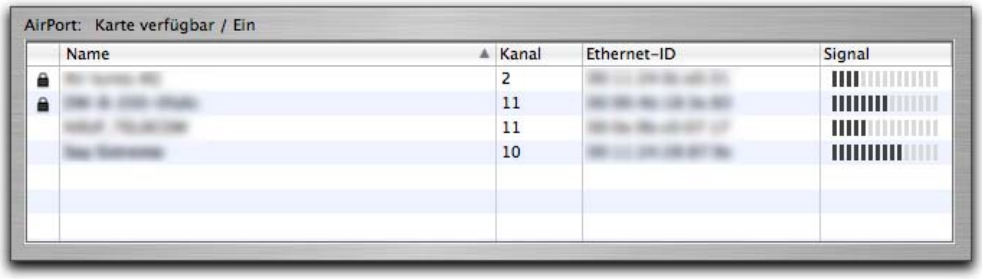
Wenn Sie die Option „IP-Adresse in die Zwischenablage kopieren“ wählen, wird Ihre IP-Adresse in die Zwischenablage kopiert und Sie können diese dann anschließend in andere Anwendungen einfügen.

Wenn Sie aus dem Popup-Menü des Etiketts „IP-Adresse“, „Subnetzmaske“, „Ethernet-ID“ oder „Schnittstelle“ die Option „Große Schrift“ wählen, werden die entsprechenden Informationen vor dem Hauptfenster von Intego NetBarrier X4 in größerer Schrift als gewöhnlich angezeigt. Wenn Sie die Anzeige abschalten wollen, müssen Sie nur auf eine beliebige Position des Fensters klicken.

AirPort

Im unteren Teil des Fensterabschnitts „Netzwerk“ erhalten Sie einen Überblick über die drahtlosen und AirPort-Netzwerke, die in der Umgebung Ihres Computers zur

Verfügung stehen – sofern Ihr Computer über eine AirPort-Karte verfügt und AirPort aktiviert ist. Ist dies nicht der Fall, werden Ihnen diese Netzwerke nicht angezeigt.



Die Liste besteht aus fünf Spalten. Sie können die Sortierungsreihenfolge der Liste ändern, indem Sie auf die Spaltenüberschriften klicken.

Die erste Spalte in diesem Abschnitt enthält entweder ein Vorhängeschloss oder sie ist leer. Wenn ein Vorhängeschloss angezeigt wird, ist der Zugriff auf dieses AirPort-Netzwerk geschützt. Sie benötigen in diesem Fall ein Passwort, um sich mit diesem Netzwerk verbinden zu können. Wenn kein Vorhängeschloss angezeigt wird, wird dieses Netzwerk nicht mit einem Passwort geschützt. Eventuell wird der Zugriff auf dieses Netzwerk jedoch auf andere Weise kontrolliert.

In der Spalte **Name** wird der Name des drahtlosen oder AirPort-Netzwerks angezeigt. Wenn Sie mit einem dieser Netzwerke verbunden sind, wird der Name in Fettschrift angezeigt.

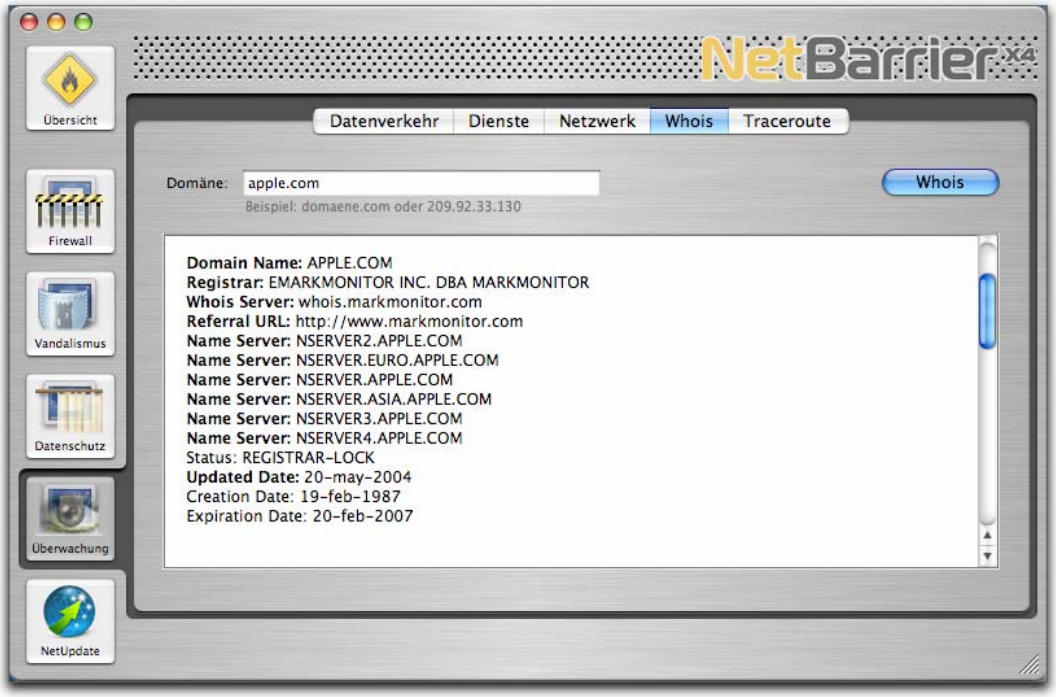
In der Spalte **Kanal** erfahren Sie, welcher Netzwerkkanal von dem drahtlosen Netzwerk verwendet wird.

In der Spalte **Ethernet-ID** wird die Ethernet-Adresse der drahtlosen oder AirPort-Basisstation angezeigt.

In der Spalte **Signal** wird die Signalstärke des Netzwerks angezeigt. Je mehr Säulen angezeigt werden, desto stärker ist das Signal, das Ihr Computer empfängt.

Whois

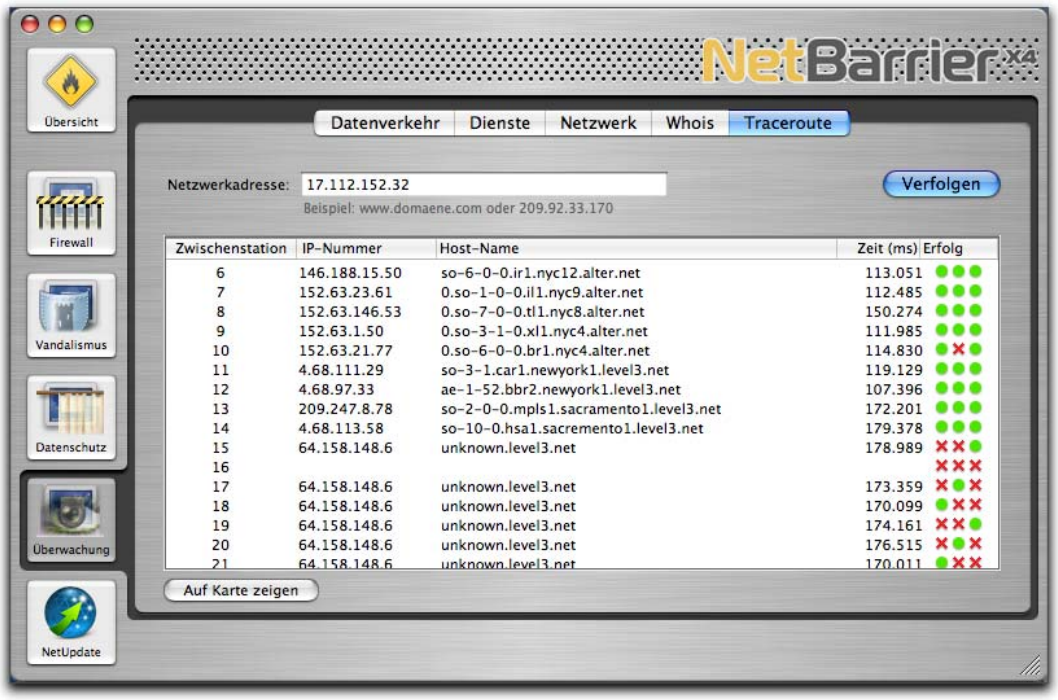
Intego NetBarrier X4 ermöglicht es Ihnen, Domänennamen und IP-Nummern unter Verwendung der integrierten Whois-Funktion aufzulösen. Geben Sie hierzu einen Domänennamen oder eine IP-Nummer ins Domänenfeld ein und klicken Sie dann auf die Schaltfläche „Whois“. Im Textfeld darunter sehen Sie nun die Informationen über die Domäne.



In Intego NetBarrier X4 sind standardmäßig fünf Whois-Server definiert. Sie können diese ändern oder weitere Whois-Server angeben. Weitere Informationen über das Hinzufügen von Whois-Servern finden Sie im Kapitel 6, **Voreinstellungen und Konfigurationen**.

Traceroute

Wenn Sie Daten ins Internet oder ein andere Netzwerk senden oder aus diesem empfangen, werden die Daten in Paketen von einem Relaisserver zu einem anderen gesendet, bis sie das Datenziel erreichen. Unter Umständen „springen“ die Daten hierbei über Dutzende dieser Relaisserver. Die in Intego NetBarrier X4 implementierte Funktion „Traceroute“ (Routenverfolgung) ermöglicht Ihnen, genau zu sehen, welchen Weg Ihre Daten durchs weltweite Datennetz genommen haben. Dies ist vor allem dann zweckmäßig, wenn ein bestimmter Server nicht erreicht werden kann. Sie können dann sehen, wo die Verbindung unterbrochen ist. Im Normalfall ist dann ein wichtiger Relaisserver oder Router außer Betrieb.

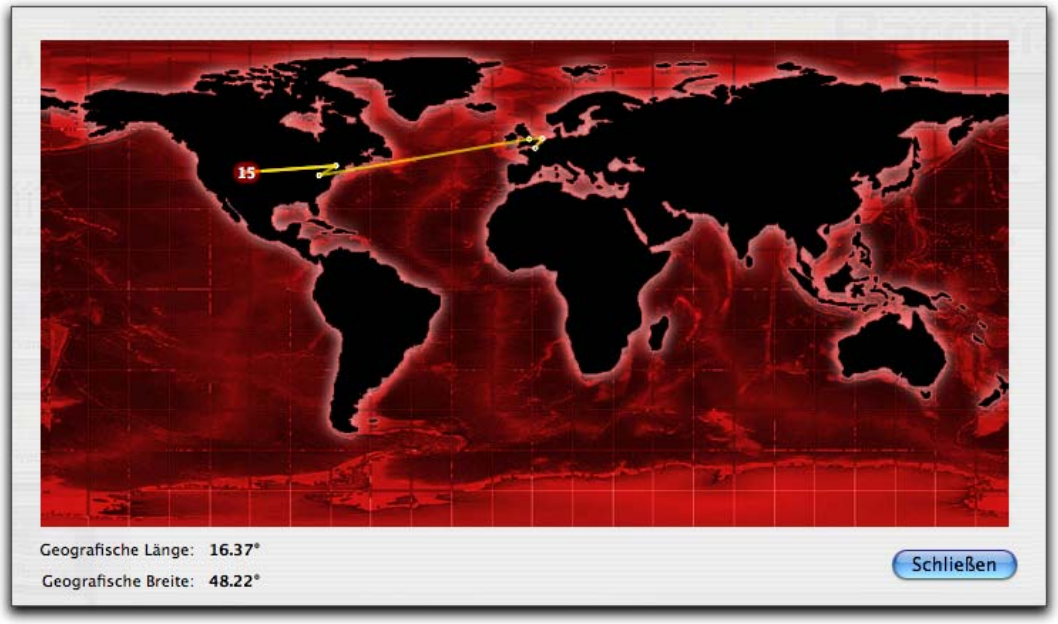


Sie können die Funktion „Traceroute“ verwenden, indem Sie eine IP-Adresse oder einen Domänennamen in das Feld „Netzwerkadresse“ eingeben und dann auf die Schaltfläche „Verfolgen“ klicken. Wenn Sie einen Domänennamen eingeben, wird

dieser von Intego NetBarrier X4 in die entsprechende IP-Adresse aufgelöst, die dann angezeigt wird.

Im Fenster „Traceroute“ werden nun alle Zwischenstationen (Relaisserver) zwischen Ihrem Computer und dem Zielserver angezeigt. Für jede Zwischenstation zeigt Intego NetBarrier X4 die laufende Nummer, die IP-Adresse, den Domänennamen, die Reaktionszeit und die Anzahl der Ping-Datentelegramme an, die erfolgreich oder nicht erfolgreich übertragen wurden. Erfolgreiche Ping-Datentelegramme werden als grüne Kreise und fehlgeschlagene Ping-Datentelegramme als rote Kreuze dargestellt. Für jede Zwischenstation sendet Intego NetBarrier X4 drei Ping-Datentelegramme. Wenn Ihr Computer über einen Router mit dem Internet verbunden ist, reagiert dieser unter Umständen nicht auf Ping-Anfragen. Hierdurch wird die Verfolgung der Ping-Datentelegramme bis zum gewünschten Zielserver jedoch nicht unmöglich gemacht.

Nach Beendigung der Funktion „Traceroute“ können Sie auf einer Weltkarte sehen, welchen Weg Ihre Ping-Datentelegramme genommen haben. Hierzu müssen Sie nur auf die Schaltfläche „Auf Karte zeigen“ klicken. Auf der Weltkarte sehen Sie nun Linien, mit denen der Zielserver über die Zwischenstationen mit Ihrem Computer verbunden ist. Hierbei werden die Nummern aller beteiligten Computer angezeigt.



Klicken Sie anschließend auf die Schaltfläche „Schließen“.

NetUpdate

NetUpdate ist ein Programm für die automatische oder manuelle Aktualisierung der auf Ihrem Macintosh installierten Intego-Software. Das Programm Intego NetUpdate wird gleichzeitig mit Intego NetBarrier X4 oder einem anderen Anwendungsprogramm von Intego installiert. Intego NetUpdate prüft sämtliche auf Ihrem Computer installierte Intego-Software auf die Verfügbarkeit neuer Versionen, die von NetUpdate automatisch heruntergeladen und installiert werden können.

Auf der Registerkarte „NetUpdate“ sehen Sie Informationen über die auf Ihrem Computer installierte Version der Intego-Software, den Zeitpunkt der letzten Prüfung auf aktualisierte Intego-Software und das Ablaufdatum Ihres Abonnements auf Intego-Softwareaktualisierungen (sofern Ihr Abonnement gültig ist). Wenn Sie nach Aktualisierungen suchen möchten, klicken Sie auf die Schaltfläche „Jetzt prüfen…“. NetUpdate startet dann und sucht nach Aktualisierungen.

Weitere Informationen über die Verwendung von NetUpdate finden Sie im zugehörigen Benutzerhandbuch.

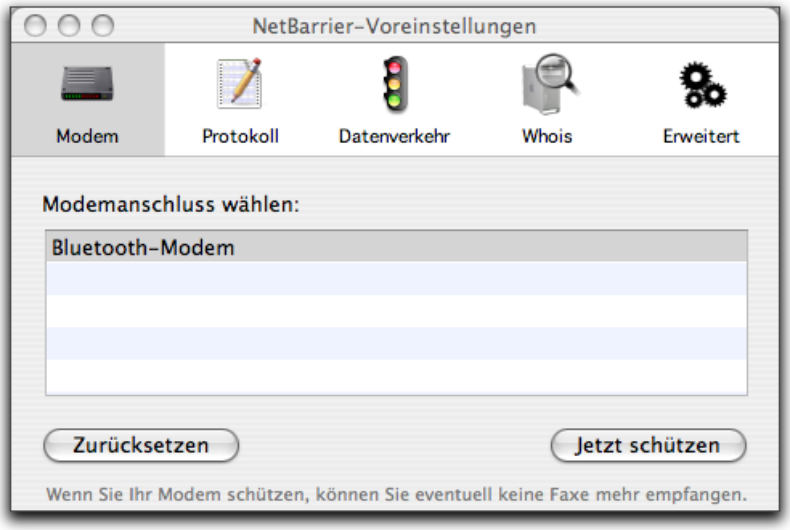
6 – Voreinstellungen und Konfigurationen

Voreinstellungen von Intego NetBarrier X4

Das Dialogfeld „NetBarrier-Voreinstellungen“ ermöglicht Ihnen das Ändern der Voreinstellungen einiger Funktionen von Intego NetBarrier X4. Wählen Sie hierzu die Option „Voreinstellungen“ aus dem Menü von Intego NetBarrier X4.

Modem

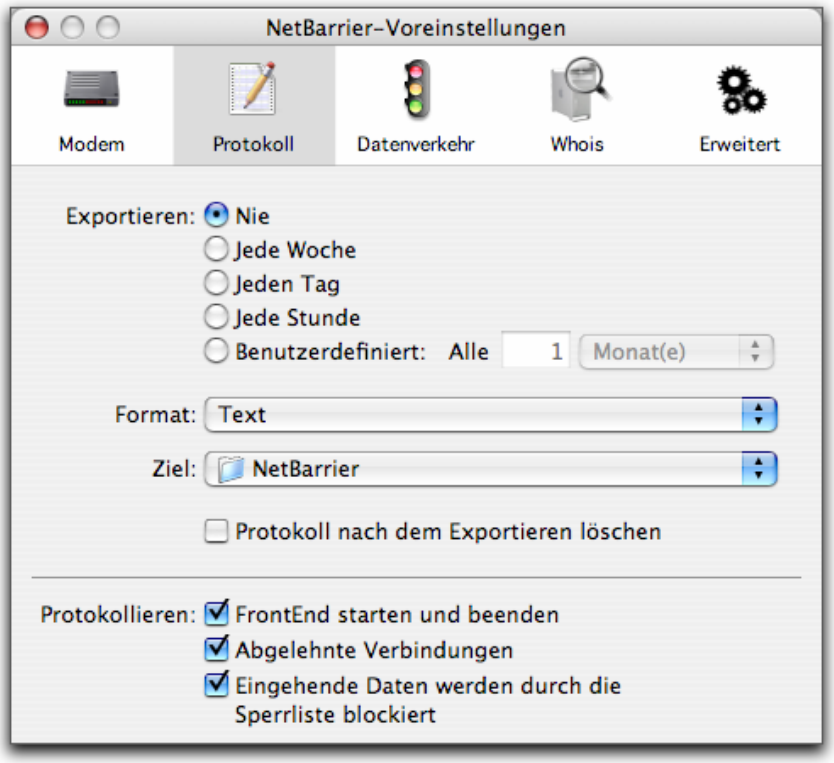
Diese Option ermöglicht es Ihnen, Ihren Modem so zu konfigurieren, dass er keine Anrufe annehmen kann. Klicken Sie hierzu im Dialogfeld „NetBarrier-Voreinstellungen“ auf die Schaltfläche „Modem“. Hierdurch kann Ihr Modem keine Anrufe mehr entgegennehmen. Klicken Sie dann auf die Schaltfläche „Jetzt sichern“. Durch Klicken auf die Schaltfläche „Zurücksetzen“ können Sie die Sicherung Ihres Modems abschalten.



Intego NetBarrier X4 konfiguriert Ihren Modem so, dass er keine Anrufe mehr entgegennehmen kann.

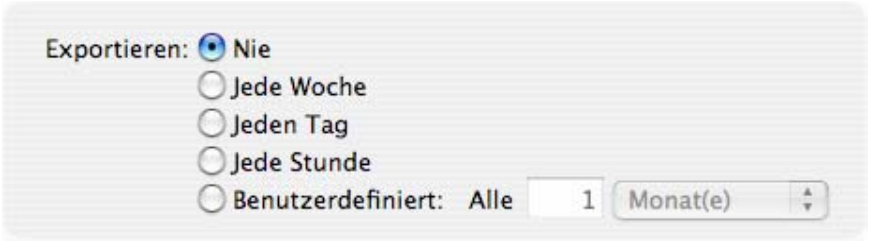
Einstellungen für Protokollexport

Sie können Intego NetBarrier X4 so konfigurieren, dass das Protokoll automatisch in von Ihnen vorgegebenen Zeitintervallen exportiert wird. Klicken Sie hierzu im Fenster „NetBarrier-Voreinstellungen“ auf die Schaltfläche „Protokoll“.



Exportieren von Protokolldaten

Wenn das Protokoll von Intego NetBarrier X4 automatisch in von Ihnen vorgegebenen Zeitintervallen exportiert werden soll, können Sie hierfür eine von 5 Optionen wählen. Standardmäßig ist die Option „Nie“ aktiviert.



Nie

Die Protokolldaten werden niemals exportiert.

Jede Woche

Die Protokolldaten werden einmal pro Woche, u.z. an jedem Montag um 00:00 Uhr, exportiert. Wenn Ihr Computer zu diesem Zeitpunkt ausgeschaltet ist, werden die Datenverkehrsdaten nach dem nächsten Neustart Ihres Computers exportiert.

Jeden Tag

Wenn Ihr Computer zu diesem Zeitpunkt ausgeschaltet ist, werden die Datenverkehrsdaten nach dem nächsten Neustart Ihres Computers exportiert.

Jede Stunde

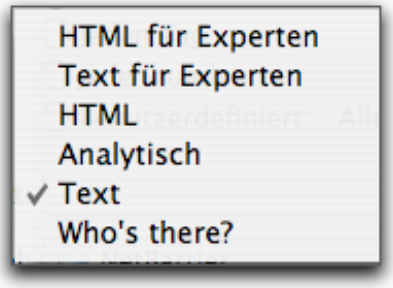
Die Protokolldaten werden einmal pro Stunde, u.z. zu jeder vollen Stunde, exportiert.

Benutzerdefiniert

Wenn dieses Kontrollkästchen markiert ist, können Sie ein beliebiges Zeitintervall fürs automatische Exportieren der Protokolldaten festlegen. Sie können beliebige Zahlenwerte (im Rahmen des Stunden- und Minutensystems) eingeben und die Zeiteinheit (Monate, Tage, Stunden und Minuten) aus dem Popup-Menü wählen.

Format der Protokolldatei

Protokolle können in sechs Formaten exportiert werden: Klicken Sie ins Popup-Menü „Format“, um das Exportformat zu wählen.



Sie haben die Auswahl aus folgenden Formaten:

HTML für Experten

Hierbei handelt es sich ums HTML-Format mit zusätzlichen Spalten. In diesem Format werden die gleichen Informationen wie im Expertenmodus angezeigt.

Text für Experten

Hierbei handelt es sich ums Textformat mit zusätzlichen Spalten. In diesem Format werden die gleichen Informationen wie im Expertenmodus angezeigt. Die Spalten werden durch Reiter separiert und können auf einfachste Weise in ein Arbeitsblatt eines Tabellenkalkulationsprogramms wie z.B. Microsoft Excel importiert werden.

HTML

Wenn Sie das Protokoll als HTML-Datei speichern, können Sie es mit jedem Webbrowser öffnen. Das Protokoll wird in Tabellenform angezeigt.

Analytisch

Dieses Format ähnelt dem Format „Text für Experten“, wobei allerdings keine Reiter vorhanden sind. Manche Felder sind beschriftet.

Text

Im Textformat exportierte Protokolle können mit jedem Textverarbeitungsprogramm verarbeitet werden.

Who’s there?

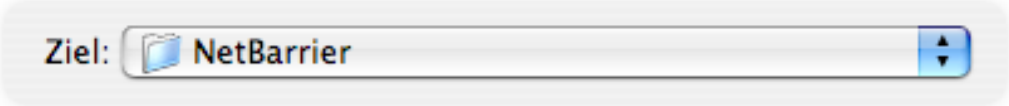
Ein in diesem (Text-)Format exportiertes Protokoll enthält folgende Informationen:

DATUM:	Datum der Verbindungsherstellung.
ZEIT:	Uhrzeit der Verbindungsherstellung.
ERGEBNIS:	Ergebnis der Verbindung.
HOSTNAME:	Die IP-Adresse des Servers.
SERVER_PORT:	Der für diese Verbindung verwendete Server-Port.
VERFAHREN:	Das verwendete Übertragungsprotokoll (TCP oder UDP).

Ziel

Sie können den Ordner wählen, in dem die Protokolldateien gespeichert werden sollen. Standardmäßig wird die Datei mit den Datenverkehrsdaten im Ordner /Library/Logs/NetBarrier gespeichert. Wenn die Datei mit den Datenverkehrsdaten in einem anderen Ordner gespeichert werden soll, müssen Sie auf die Schaltfläche „Andere…“ klicken und den gewünschten Ordner suchen. Klicken Sie dann auf die

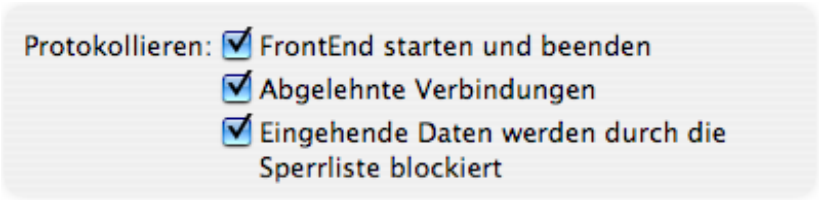
Schaltfläche „Wählen“, um diesen Ordner als Speicherort zu verwenden. Sie können auch einen neuen Ordner erstellen, indem Sie auf die Schaltfläche „Neuer Ordner“ im Dialogfeld klicken. Geben Sie diesem neuen Ordner den gewünschten Namen und klicken Sie dann auf die Schaltfläche „Erstellen“.



Anmerkung: Wenn Sie Webfreigabe verwenden, können Sie die Protokolldatei auch in einen Ordner für gemeinsame Verwendung exportieren, sodass von einem anderen Computer darauf zugegriffen werden kann.

Optionen für die Protokollierung

Das Protokoll von Intego NetBarrier X4 enthält eine Vielzahl von Informationen. Sie können jedoch festlegen, welche Informationen auf der Registerkarte „Protokoll“ angezeigt werden sollen. Wenn Sie definieren wollen, welche Informationen im Protokoll exportiert werden sollen, wählen Sie bitte eine der drei folgenden Optionen:



FrontEnd starten und beenden

Wenn Sie diese Option gewählt haben, werden generelle Aktivitäten von Intego NetBarrier X4 wie das Starten und Beenden des Programms protokolliert.

Abgelehnte Verbindungen

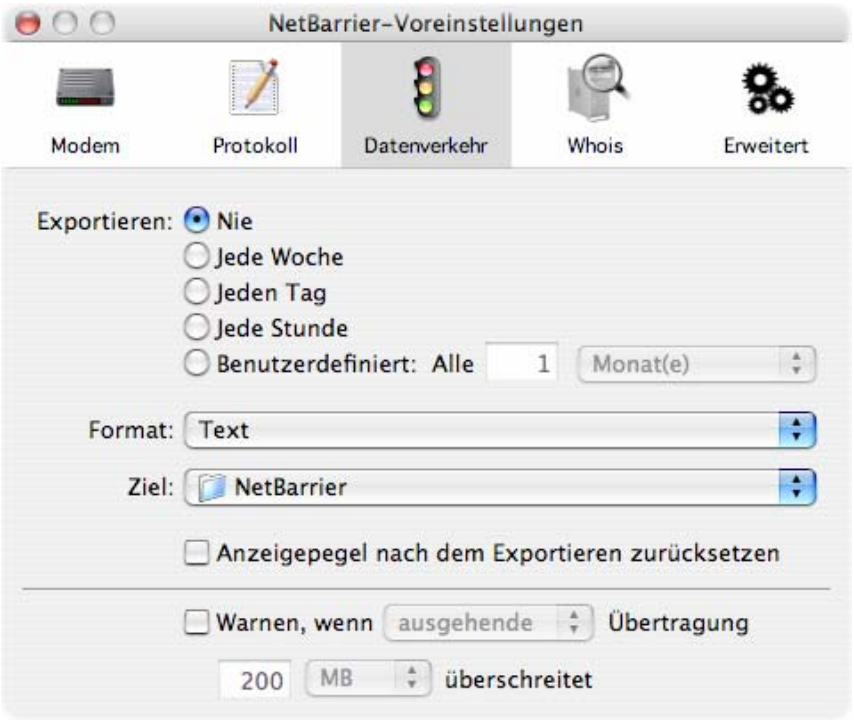
Wenn Sie diese Option gewählt haben, werden alle verweigerten Verbindungen protokolliert.

Eingehende Daten werden durch die Sperrliste blockiert

Wenn Sie diese Option gewählt haben, werden alle eingehenden Daten, Angriffe und Eindringversuche gemäß Sperrliste protokolliert.

Einstellungen für Datenverkehrexport

Sie können Intego NetBarrier X4 so konfigurieren, dass die Datenverkehrsdaten automatisch in von Ihnen vorgegebenen Zeitintervallen exportiert werden. Klicken Sie hierzu im Fenster „NetBarrier-Voreinstellungen“ auf die Schaltfläche „Datenverkehr“. Im nun geöffneten Fenster können Sie festlegen, wann und wie die Datenverkehrsdaten exportiert und verwaltet werden sollen.



Exportieren

Wenn die Datenverkehrsdaten von Intego NetBarrier X4 automatisch in von Ihnen vorgegebenen Zeitintervallen exportiert werden sollen, können Sie hierfür eine von 5 Optionen wählen. Standardmäßig ist die Option „Nie“ aktiviert.

Nie

Die Datenverkehrsdaten werden niemals exportiert.

Jede Woche

Die Datenverkehrsdaten werden einmal pro Woche, u.z. an jedem Montag um 00:00 Uhr, exportiert. Wenn Ihr Computer zu diesem Zeitpunkt ausgeschaltet ist, werden die Datenverkehrsdaten nach dem nächsten Neustart Ihres Computers exportiert.

Jeden Tag

Wenn Ihr Computer zu diesem Zeitpunkt ausgeschaltet ist, werden die Datenverkehrsdaten nach dem nächsten Neustart Ihres Computers exportiert.

Jede Stunde

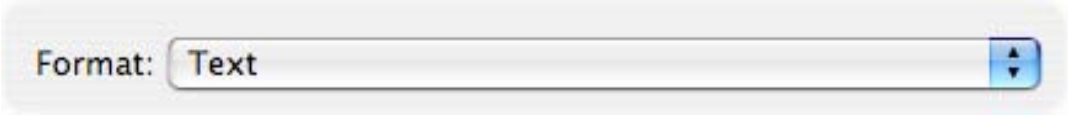
Die Datenverkehrsdaten werden einmal pro Stunde, u.z. zu jeder vollen Stunde, exportiert.

Benutzerdefiniert

Wenn dieses runde Optionsfeld markiert ist, können Sie ein beliebiges Zeitintervall fürs automatische Exportieren der Datenverkehrsdaten festlegen. Sie können beliebige Zahlenwerte (im Rahmen des Stunden- und Minutensystems) eingeben und die Zeiteinheit (Monate, Tage, Stunden und Minuten) aus dem Popup-Menü wählen.

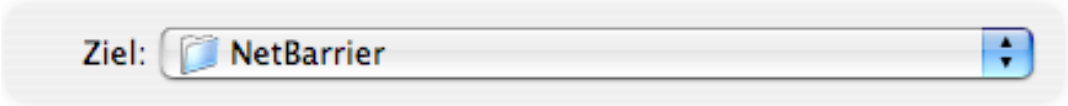
Format der Datei mit den Datenverkehrsdaten

Datenverkehrsdaten können in zwei Formaten exportiert werden: Als Text- oder HTML-Datei. Wenn Sie die Datenverkehrsdaten als Textdatei speichern, können Sie die Datei mit jedem Textverarbeitungsprogramm öffnen. Wenn Sie das Protokoll als HTML-Datei speichern, können Sie es mit jedem Webbrowser öffnen. Das Protokoll wird in Tabellenform angezeigt.



Speicherort für die Datei mit den Datenverkehrsdaten

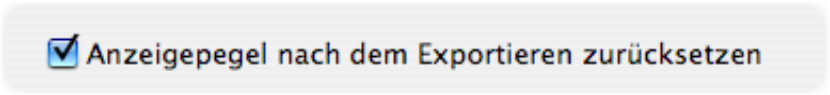
Sie können den Ordner wählen, in dem die Datei mit den Datenverkehrsdaten gespeichert werden soll. Standardmäßig wird die Datei mit den Datenverkehrsdaten im Ordner /Library/Logs/NetBarrier gespeichert. Wenn die Datei mit den Datenverkehrsdaten in einem anderen Ordner gespeichert werden soll, müssen Sie auf die Schaltfläche „Wählen…“ klicken und den gewünschten Ordner suchen. Klicken Sie dann auf die Schaltfläche „Wählen“, um diesen Ordner als Speicherort zu verwenden. Sie können auch einen neuen Ordner erstellen, indem Sie auf die Schaltfläche „Neuer Ordner“ im Dialogfeld klicken. Geben Sie diesem neuen Ordner den gewünschten Namen und klicken Sie dann auf die Schaltfläche „Erstellen“.



Anmerkung: Wenn Sie Webfreigabe verwenden, können Sie die Datei mit den Datenverkehrsdaten auch in einen Ordner für gemeinsame Verwendung exportieren, sodass von einem anderen Computer darauf zugegriffen werden kann.

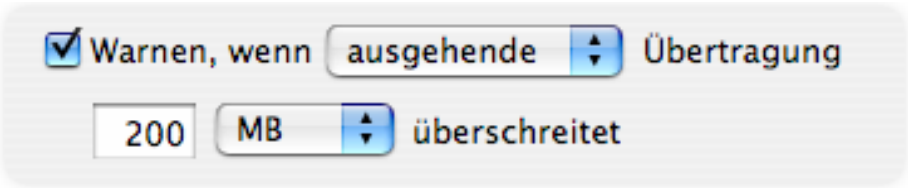
Anzeigepegel nach dem Exportieren zurücksetzen

Wenn dieses Kontrollkästchen markiert ist, werden die Messskalen zur Anzeige der Netzwerkaktivitäten nach jedem Export auf Null zurückgesetzt.



Alarm bei zu großer Datenmenge

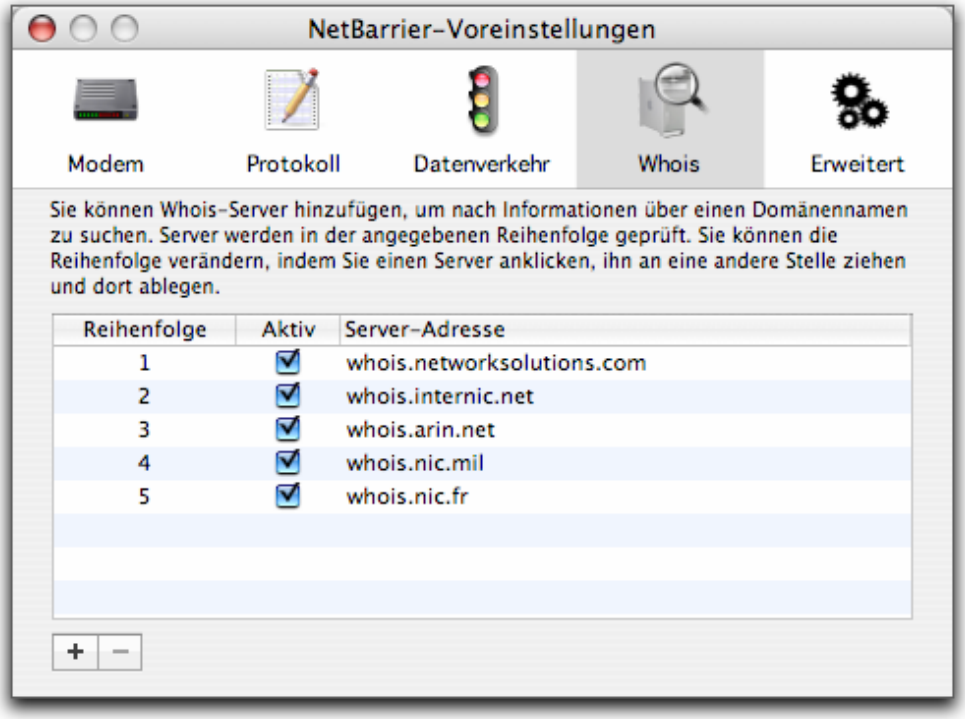
Intego NetBarrier X4 kann Sie darüber informieren, dass das IP-Datenverkehrsaufkommen in ein- oder ausgehender Richtung einen vorgegebenen Grenzwert überschreitet. Diese Funktion ist sehr nützlich, wenn das Datenverkehrsaufkommen (Datenvolumen, Datenmenge) Ihres Internet-Zugangs für gesendete und/oder empfangene Daten begrenzt ist.



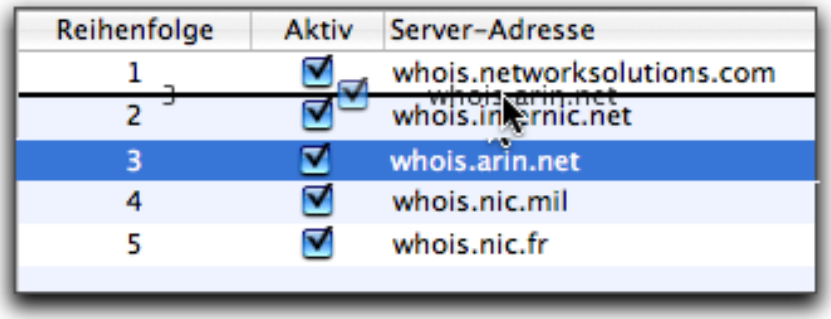
Wenn Sie das Kontrollkästchen „Warnen, wenn:“ markiert haben, gibt Intego NetBarrier X4 eine Warnmeldung aus, sobald das Datenverkehrsaufkommen Ihres Computers den vorgegebenen Grenzwert überschritten hat. Sie können festlegen, ob die Alarmgabe bei ein- und/oder ausgehendem Datenverkehr erfolgen soll. Sie können den Grenzwert in Kilobyte, Megabyte oder Gigabyte angeben.

Whois

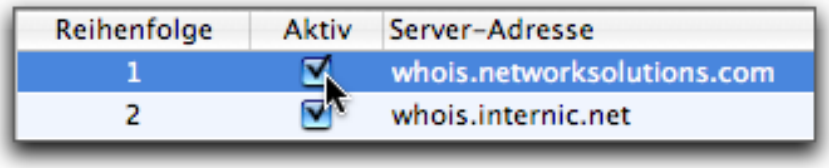
Die Whois-Funktion von Intego NetBarrier X4 ermöglicht es Ihnen, den Domänennamen oder die IP-Adresse suchen zu lassen. In diesem Dialogfeld sind bereits vier Whois-Server vordefiniert, die in der angezeigten Reihenfolge abgefragt werden.



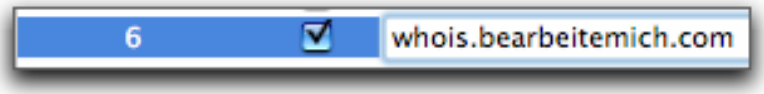
Sie können die Reihenfolge der Abfrage ändern, indem Sie auf den Domänennamen des betreffenden Whois-Servers klicken und diesen dann in die gewünschte Position ziehen.



Sie können die Whois-Server in diesem Fenster aktivieren oder abschalten. Um einen Whois-Server abzuschalten, müssen Sie die Markierung aus dem Kontrollkästchen links von seiner Adresse entfernen. Um einen abgeschalteten Whois-Server wieder zu aktivieren, müssen Sie das Kontrollkästchen links von seinem URL markieren.



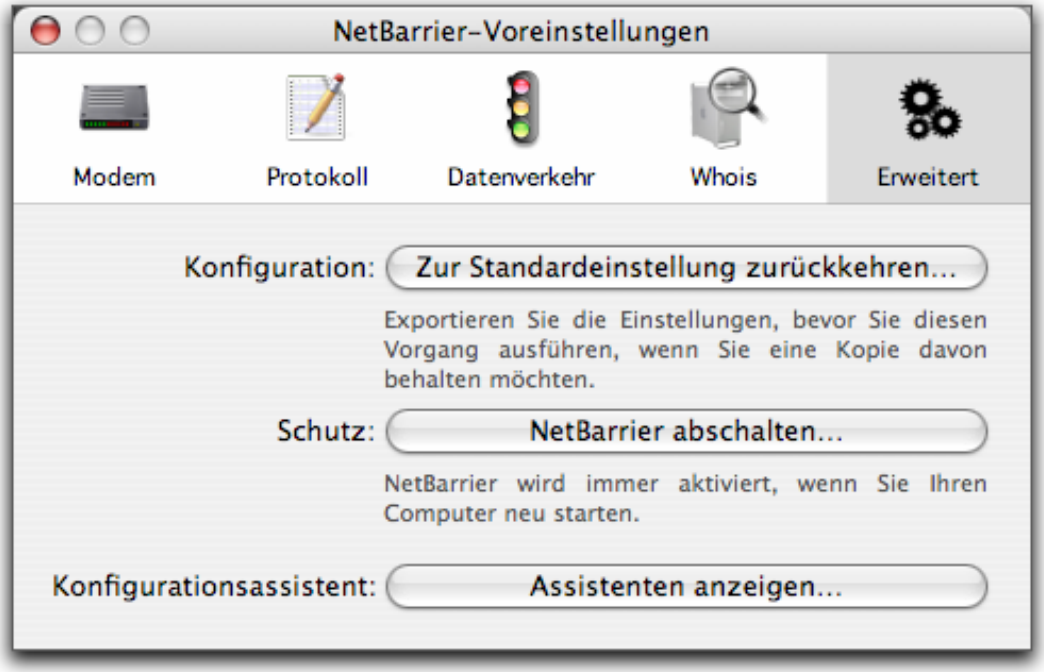
Sie können auch neue Whois-Server hinzufügen. Klicken Sie hierzu auf die Schaltfläche „+“. Der Liste wird dann eine neue Zeile mit einer hervorgehobenen Muster-Serveradresse hinzugefügt. Geben Sie nun den Namen des neuen Whois-Servers ins Feld für die Serveradresse ein.



Wenn Sie einen Whois-Server entfernen möchten, klicken Sie zur Auswahl auf den entsprechenden Server und anschließend auf die Schaltfläche „-“. Nun wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, den Löschvorgang zu bestätigen oder abzubrechen.

Erweiterte Optionen

Im Fensterabschnitt „Erweitert“ in den Voreinstellungen für NetBarrier stehen Ihnen drei Optionen zur Auswahl.



Konfiguration

Wenn Sie auf die Schaltfläche „Zur Standardeinstellung zurückkehren…“ klicken, wird NetBarrier X4 auf die Standard-Konfiguration zurückgesetzt: Client, lokaler Server-Modus für die Firewall und die Antivandalismus- sowie Datenschutzfunktionen sind deaktiviert. Um diese Konfiguration aktivieren zu können, benötigen Sie ein Administratorkennwort. Wir empfehlen Ihnen, Ihre aktuellen Einstellungen für

NetBarrier X4 zu exportieren (Ablage > Voreinstellungen exportieren…), bevor Sie zu den Standardeinstellungen zurückkehren, falls Sie diese Einstellungen später erneut verwenden möchten.

Schutz

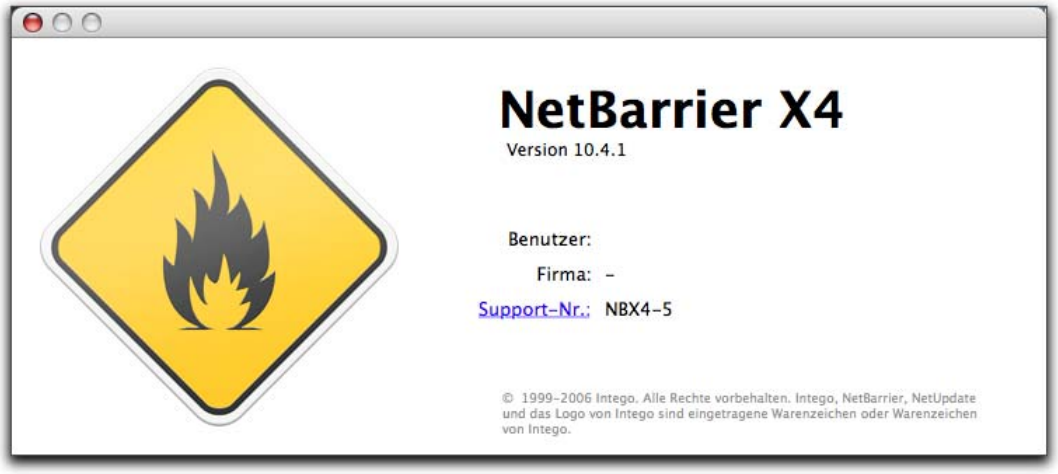
Wenn Sie auf die Schaltfläche „NetBarrier abschalten…“ klicken, wird NetBarrier X4 vollständig abgeschaltet – einschließlich der Protokollfunktion. Hierzu benötigen Sie ein Administratorkennwort. Sobald NetBarrier X4 abgeschaltet ist, wechselt die Schaltfläche auf „NetBarrier aktivieren…“. Wenn Sie NetBarrier wieder einschalten möchten, klicken Sie auf die Schaltfläche und geben Sie noch einmal ein Administratorkennwort ein. Wenn Sie Ihren Computer neu starten wird NetBarrier X4 automatisch eingeschaltet.

Konfigurationsassistent

Wenn Sie auf die Schaltfläche „Assistenten anzeigen…“ klicken, wird der Konfigurationsassistent von NetBarrier X4 gestartet. Weitere Informationen hierzu erhalten Sie in Kapitel 4, **Erste Schritte**.

Über Intego NetBarrier X4

Wenn Sie die Option „Über NetBarrier X4“ aus dem Menü von NetBarrier wählen, wird ein Fenster geöffnet, in dem Ihnen einige Informationen über Intego NetBarrier X4 angezeigt werden - beispielsweise die Versionsnummer und Ihre Support-Nummer (eine Nummer, die Sie für die technische Kundenunterstützung benötigen).


NetBarrier X4
Version 10.4.1
Benutzer:
Firma: -
Support-Nr.: NBX4-5
© 1999-2006 Intego. Alle Rechte vorbehalten. Intego, NetBarrier, NetUpdate und das Logo von Intego sind eingetragene Warenzeichen oder Warenzeichen von Intego.

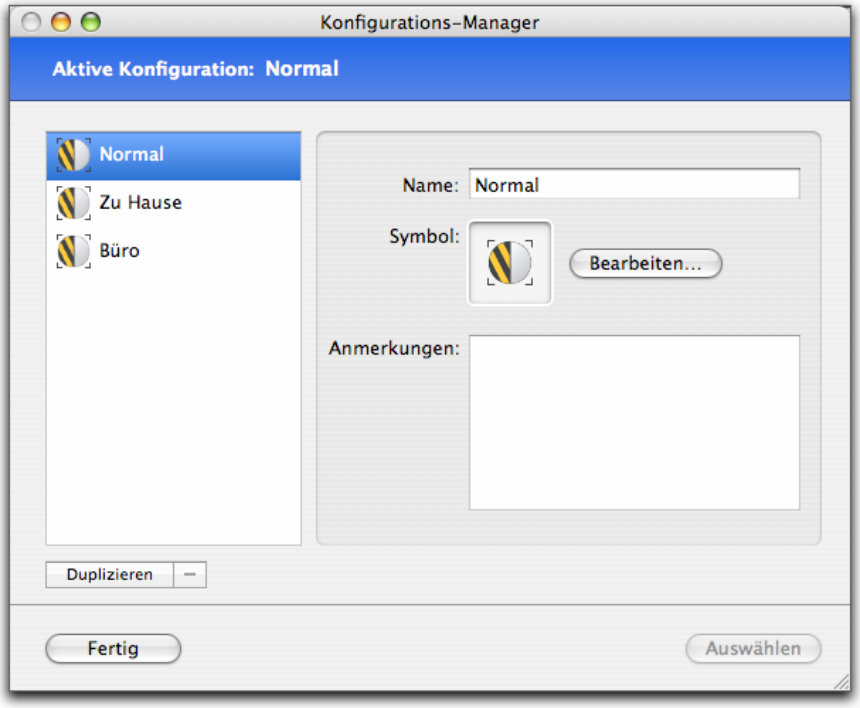
Wenn Sie auf den Link „Support-Nr.“ Klicken, können Sie eine E-Mail-Nachricht an die Technische Kundenunterstützung von Intego schreiben.

Konfigurations-Manager

Intego NetBarrier X4 bietet Ihnen die Möglichkeit zum Speichern beliebig vieler Konfigurationssätze. Jeder Konfigurationssatz besteht aus allen Voreinstellungen von Intego NetBarrier X4. Sie können Konfigurationssätze für verschiedene Orte definieren. Dies ist beispielsweise dann zweckmäßig, wenn Sie ein Laptop besitzen, das Sie zuhause und im Büro verwenden. Unter Umständen wollen Sie einen Konfigurationssatz mit zusätzlichem Schutz verwenden, wenn Sie Ihren Computer als Server einsetzen, während ein anderer Konfigurationssatz verwendet wird, wenn Ihr Computer nur als Client arbeitet. Sie können beispielsweise auch einen eigenen Konfigurationssatz speichern, den Sie verwenden, wenn Ihr Computer nur in ein Netzwerk integriert, aber nicht mit dem Internet verbunden ist. Ein anderer Konfigurationssatz bietet zusätzlichen Schutz, wenn Sie mit Ihrem Computer im World Wide Web surfen. Es kann auch zweckmäßig sein, einen Konfigurationssatz zu definieren und zu speichern, in dem Sie festgelegt haben, dass Intego NetBarrier X4 Ihnen eine E-Mail-Mitteilung schicken soll, sobald ein Eindringversuch erkannt wurde, wenn Sie nicht in der Nähe Ihres Computers sind.

Auswählen der aktiven Konfiguration

Um einen Konfigurationssatz zu wählen, müssen Sie aus dem Menü „Ablage“ die Menüoption „Konfigurationen…“ wählen. Nun wird ein Dialogfeld geöffnet.

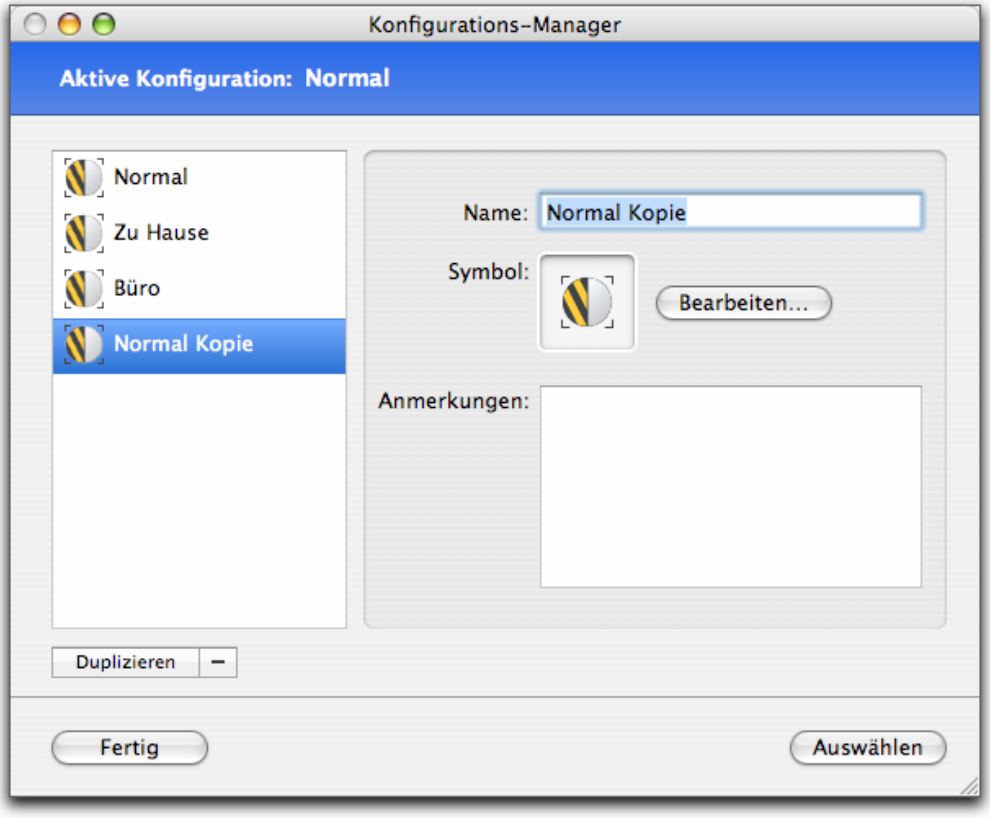


Wählen Sie den zu aktivierenden Konfigurationssatz und klicken Sie dann auf die Schaltfläche „Auswählen“. Wenn Sie diesen Konfigurationssatz dann doch nicht aktivieren wollen, müssen Sie nur auf die Schaltfläche „Fertig“ klicken oder einen anderen Konfigurationssatz wählen.

Hinzufügen von Konfigurationssätzen

Um einen Konfigurationssatz hinzuzufügen, müssen Sie aus dem Menü „Ablage“ die Menüoption „Konfigurationen…“ wählen. Nun wird ein Dialogfeld geöffnet.

Um einen neuen Konfigurationssatz erstellen zu können, müssen Sie zunächst einen bereits vorhandenen Konfigurationssatz kopieren und der Kopie einen eigenen Namen geben. Klicken Sie hierzu auf den Namen eines der Konfigurationssätze in der Liste und dann auf die Schaltfläche „Duplizieren…“. Hierauf wird in der Liste eine neue Konfiguration angezeigt:



Geben Sie den Namen für Ihren neuen Konfigurationssatz ein. Wenn Sie das Symbol ändern möchten, klicken Sie auf die Schaltfläche „Bearbeiten…“ und suchen Sie das Bild, das Sie als Symbol für diesen Satz verwenden möchten. Im Abschnitt „Anmerkungen“ können Sie Informationen zu dieser Konfiguration hinzufügen.

Jetzt können Sie den neuen Konfigurationssatz aktivieren, indem Sie auf die Schaltfläche „Auswählen“ klicken. Der Konfigurations-Manager wird geschlossen.

Anschließend können Sie die Konfiguration von NetBarrier X4 beliebig verändern und als aktuellen Konfigurationssatz speichern. Wenn Sie einen anderen Konfigurationssatz verwenden wollen, öffnen Sie den Konfigurations-Manager und wählen Sie ihn aus der Liste der Konfigurationssätze. Sie können auch einen anderen Konfigurationssatz aus der Konfigurationsliste im Intego-Menü in der Menüzeile wählen.

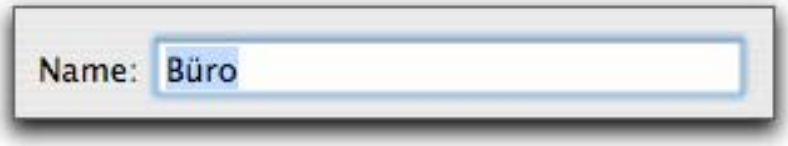
Löschen von Konfigurationssätzen

Um einen Konfigurationssatz zu löschen, müssen Sie aus dem Menü „Ablage“ die Menüoption „Konfigurationen…“ wählen. Nun wird ein Dialogfeld geöffnet. Wählen Sie einen Konfigurationssatz, indem Sie auf einen der Sätze in der Liste klicken. Klicken Sie anschließend auf die Schaltfläche „-“ in der unteren linken Ecke.

Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie den Konfigurationssatz wirklich löschen wollen. Klicken Sie auf „Entfernen“. Wenn Sie den Konfigurationssatz doch nicht löschen wollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.

Umbenennen von Konfigurationssätzen

Um einen Konfigurationssatz umzubenennen, müssen Sie aus dem Menü „Ablage“ die Menüoption „Konfigurationen…“ wählen. Nun wird ein Dialogfeld geöffnet. Wählen Sie einen Konfigurationssatz aus, indem Sie auf einen Satz in der Liste klicken und geben Sie den neuen Namen in das Namensfeld auf der rechten Seite ein.

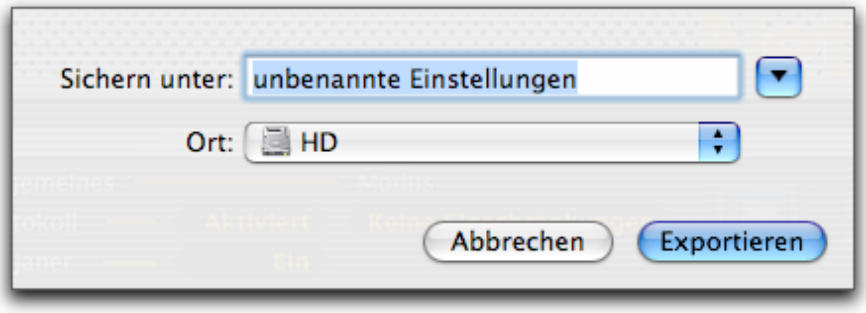


Tippen Sie den neuen Namen für Ihren Konfigurationssatz ein und drücken Sie anschließend die Eingabetaste. Wenn Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf „Fertig“, um den Konfigurations-Manager zu verlassen.

Exportieren von Voreinstellungen

Sie können Ihre Voreinstellungen von Intego NetBarrier X4 in einer Datei speichern, aus der Sie die Voreinstellungen auf einem anderen Computer mit installiertem Intego NetBarrier X4 importieren können. Dies ist vor allem dann zweckmäßig, wenn Sie mehrere Computer verwalten und für alle Computer die gleichen Voreinstellungen verwenden wollen.

Wählen Sie zum Exportieren der Einstellungen „Ablage“ > „Voreinstellungen exportieren…“ aus. Daraufhin werden Sie in einem Dialogfeld aufgefordert, einen Namen für die Datei mit den Einstellungen einzugeben und einen Speicherort zu wählen. Klicken Sie auf „Exportieren“, wenn Sie fertig sind.



Importieren von Voreinstellungen

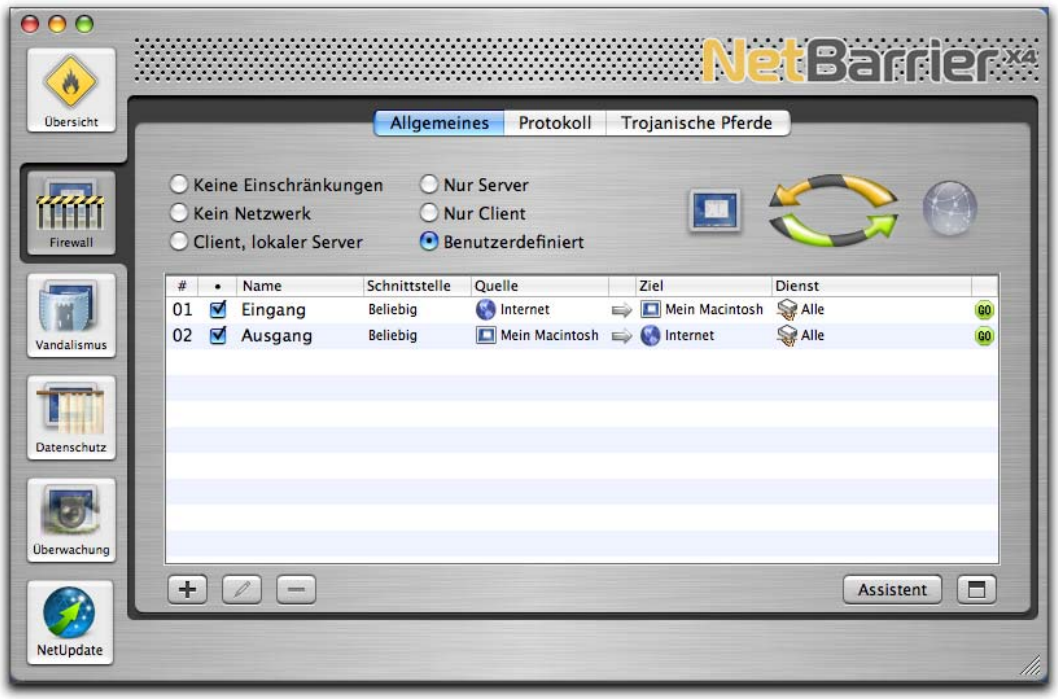
Wenn Sie Voreinstellungen von einer Kopie von Intego NetBarrier X4 (siehe oben) exportiert haben, können Sie diese in eine andere Kopie der Software importieren.

Wählen Sie hierzu die Option „Ablage“ > „Voreinstellungen importieren…“. Nun wird ein Dialogfeld geöffnet, in dem Sie aufgefordert werden, die Datei mit den Voreinstellungen zu suchen. Wenn Sie die Datei gefunden haben, klicken Sie auf „Importieren“. Diese Einstellungen werden dann sofort auf Intego NetBarrier X4 angewendet.

7 – Individuell konfigurierter Schutz

Verwenden des Modus „Benutzerdefiniert“ von Intego NetBarrier X4

Im Modus „Benutzerdefiniert“ stehen Ihnen zusätzliche Optionen für die Firewall von Intego NetBarrier X4 zur Verfügung. Alle anderen Funktionen bleiben die gleichen wie bis zu dieser Stelle im vorliegenden Benutzerhandbuch beschrieben.



Der Modus „Benutzerdefiniert“ ermöglicht die Verwendung der leistungsfähigsten Funktionen von Intego NetBarrier X4. In diesem Modus können Sie die Firewall-Regeln von Intego NetBarrier X4 selbst nach Ihren Wünschen definieren.

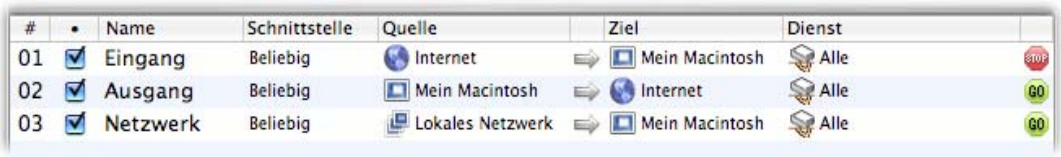
WICHTIG: Der Modus „Benutzerdefiniert“ von Intego NetBarrier X4 sollte nur von erfahrenen Netzwerkverwaltern verwendet werden. Durch fehlerhafte Einstellungen kann der Netzwerkzugriff durch Ihren Computer beeinträchtigt werden.

Vom Benutzer konfigurierbare Firewall-Optionen

Die in Intego NetBarrier X4 integrierte Firewall ermöglicht es Ihnen, eigene Firewall-Regeln zu definieren, nach denen ein- und ausgehende Datenpakete auf spezielle Datenquellen, Datenziele und Dienste geprüft werden. Nach der Prüfung werden die von Ihnen vorgegebenen Aktionen durchgeführt. Ihre selbst definierten Firewall-Regeln können grob sein, sodass beispielsweise jeder eingehende Datenverkehr gesperrt wird. Sie können auch sehr präzise definiert sein, sodass beispielsweise nur der Empfang von Datenpaketen durch Ihren Computer gesperrt wird, die von einem Computer mit einer bestimmten Internet-Adresse unter Nutzung eines bestimmten Dienstes an Ihren Computer gesendet werden.

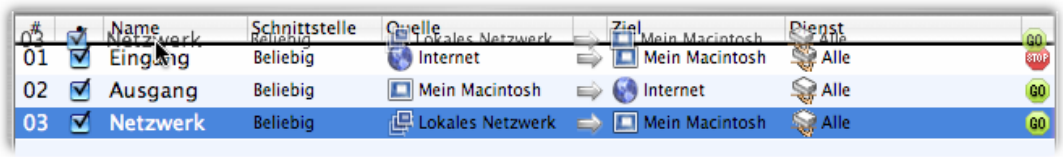
Reihenfolge der Firewall-Regeln

Die Firewall-Regeln werden in der Reihenfolge angewandt, in der sie in der Liste angezeigt werden. Aus diesem Grund sollten Sie sicherstellen, dass die von Ihnen definierten Firewall-Regeln die korrekte Reihenfolge haben, um die gewünschten Funktionen zu erfüllen.



Im vorstehenden Beispiel sperrt die erste Regel vom Internet eingehende Datenpakete. Hiervon sind auch Daten betroffen, die über ein anderes Netzwerk wie z.B. ein LAN (Local Area Network = lokales Netzwerk) bei Ihrem Computer eingehen. Die Regel 3 lässt eingehende Datenpakete von einem lokalen Netzwerk zu. Da diese Regel jedoch die dritte Regel ist, wird sie nicht wirksam, da ihr die Regel 1 widerspricht. Damit die Regel 3 angewandt werden kann, muss sie in der Liste nach oben verschoben werden.

Wählen Sie hierzu die gewünschte Regel und schieben Sie diese mit der Maus in die gewünschte Position in der Liste.



Definieren von Regeln mit dem Regelassistenten

In Intego NetBarrier X4 ist ein Regelassistent implementiert, der Sie dabei unterstützt, Ihre eigenen Firewall-Regeln zu definieren. Dank diesem Assistenten werden hierfür nur wenige Mausklicks benötigt. Mit dem Regelassistenten können Sie zwar nicht auf alle Regeln von Intego NetBarrier X4 zugreifen, doch decken die damit definierbaren Regeln die meisten Anwendungsfälle ab. Wenn Sie eine weitergehende Anpassung an Ihre Anforderungen wünschen, können Sie die Regeln zunächst mit dem Regelassistenten definieren und anschließend manuell modifizieren.

Der Regelassistent von Intego NetBarrier X4 führt Sie durch mehrere Schritte zur Definition einer Regel:

- **Name und Verhalten**
- **Richtung**
- **Dienst**
- **Dauer**
- **Optionen**
- **Beenden**

Wenn Sie eine neue Regel definieren wollen, müssen Sie auf die Schaltfläche „Assistent“ klicken.

Hierauf wird das erste Dialogfeld des Regelassistenten geöffnet.

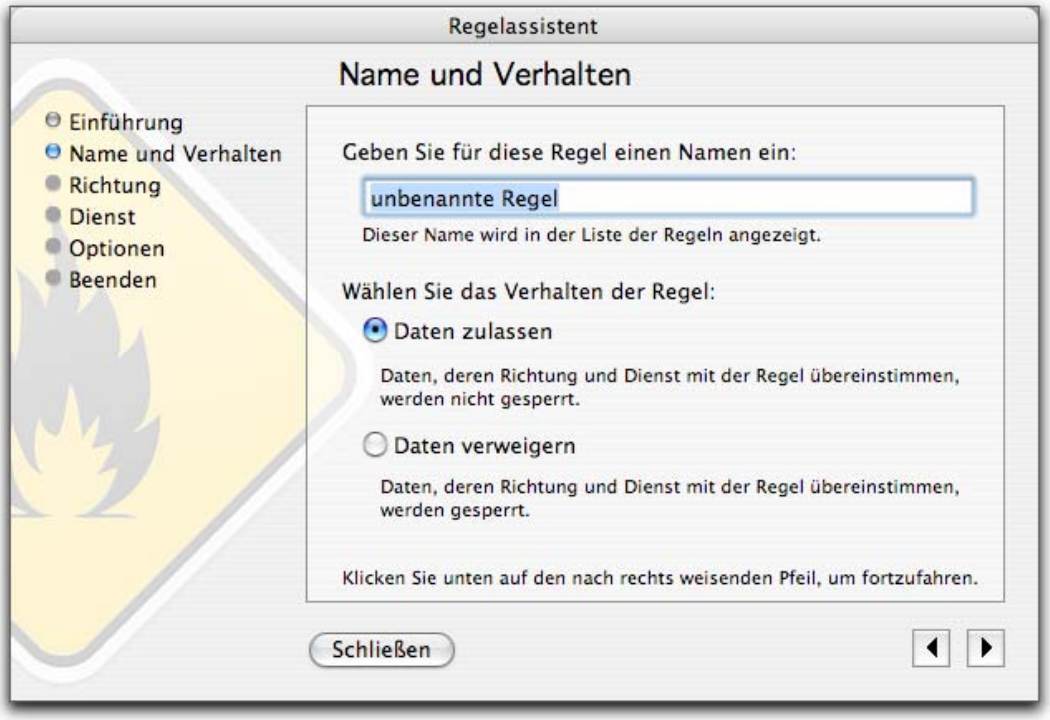
Regelassistent
Einführung
Einführung
Name und Verhalten
Richtung
Dienst
Optionen
Beenden
Dieser Assistent führt Sie durch die Schritte zum Definieren einer Firewall-Regel.
Wenn Sie eine weitergehende Anpassung wünschen oder Ihre Regeln ändern wollen, müssen Sie die Regeln manuell ändern.
Klicken Sie zunächst auf den nach rechts weisenden Pfeil.
Schließen

Klicken Sie auf den nach rechts weisenden Pfeil, um mit dem Definieren der Regel zu beginnen. Klicken Sie auf den nach links weisenden Pfeil, um wieder die vorigen Dialogfelder zu öffnen.

Alternativ können Sie auf „Schließen“ klicken, um den Regelassistenten zu beenden.

Name und Verhalten

In diesem Dialogfeld können Sie Ihrer neuen Regel einen Namen geben.

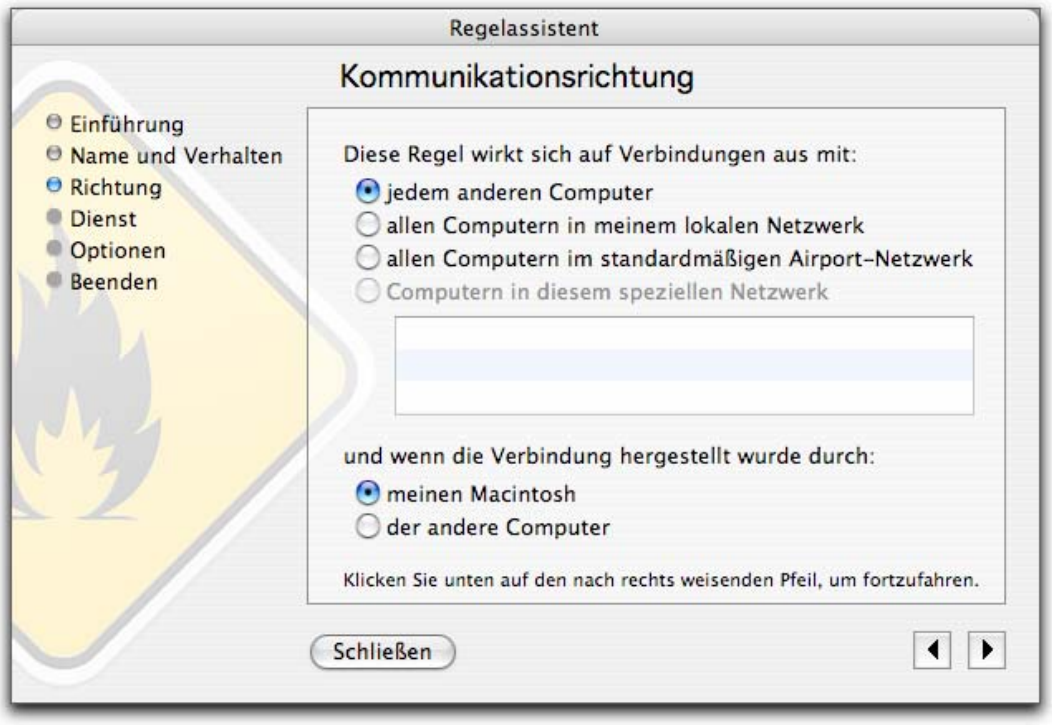

Regelassistent
Name und Verhalten
Einführung
Name und Verhalten
Richtung
Dienst
Optionen
Beenden
Geben Sie für diese Regel einen Namen ein:
unbenannte Regel
Dieser Name wird in der Liste der Regeln angezeigt.
Wählen Sie das Verhalten der Regel:
Daten zulassen
Daten, deren Richtung und Dienst mit der Regel übereinstimmen, werden nicht gesperrt.
Daten verweigern
Daten, deren Richtung und Dienst mit der Regel übereinstimmen, werden gesperrt.
Klicken Sie unten auf den nach rechts weisenden Pfeil, um fortzufahren.
Schließen

Geben Sie einen Namen ins entsprechende Feld ein und wählen Sie das Verhalten der neuen Regel: „Daten zulassen“ oder „Daten verweigern“. Wenn Sie die Option „Daten zulassen“ gewählt haben, gibt die Regel die Daten gemäß Transportrichtung und Dienst frei. Wenn Sie die Option „Daten verweigern“ gewählt haben, sperrt die Regel die Daten gemäß Transportrichtung und Dienst.

Klicken Sie auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

Kommunikationsrichtung

In diesem Dialogfeld können Sie die Richtung des Datentransfers und den Computer wählen, von dem die Verbindung hergestellt wird.



Wählen Sie zuerst im Abschnitt „Diese Regel wirkt sich auf Verbindungen aus mit:“ einen entfernten Server aus. Für die Auswahl des entfernten Servers bestehen vier Möglichkeiten:

Jedem anderen Computer
Hierbei handelt es sich um jeden anderen Computer als Ihren Computer.

Computern in meinem lokalen Netzwerk
Hierbei handelt es sich um jeden anderen Computer im gleichen Netzwerk, mit dem auch Ihr Macintosh verbunden ist.

Computern im standardmäßigen Airport-Netzwerk
Hierbei handelt es sich um jeden Computer, der mit Ihrem standardmäßigen AirPort-Netzwerk (sofern vorhanden) verbunden ist.

Computern in diesem speziellen Netzwerk
Wenn Sie mit dem Regelassistenten ein spezielles Netzwerk definiert haben, können Sie dieses Netzwerk wählen.

Wählen Sie nun den Computer, von dem die Verbindung hergestellt wird:

Mein Macintosh
Hierbei handelt es sich um Ihren Macintosh, also den Computer, der diese Regel anwendet.

Der andere Computer
Hierbei handelt es sich um den entfernten Server, den Sie im ersten Abschnitt dieses Dialogfelds definiert haben.

Klicken Sie abschließend auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

Dienst

In diesem Dialogfeld können Sie den Dienst wählen, auf den sich die Regel auswirkt.

Drei Arten von Diensten stehen Ihnen zur Auswahl:

Alle Dienste

Hierbei handelt es sich um alle Netzwerkdienste.

TCP-Dienste (Verbindungsdienste)

Hierbei handelt es sich um Dienste, die eine bestehende Verbindung zwischen zwei Computern erfordern, also die Dienste HTTP, FTP, TELNET, SSH, POP3, AppleShare, usw. Dies betrifft alle TCP-Verbindungen.

Dieser Dienst

Sie haben die Auswahl aus mehreren Diensten für populäre Anwendungsprogramme und Internet-Datenübertragungsprotokolle. Klicken Sie auf den Namen des gewünschten Dienstes in der Liste.

Klicken Sie abschließend auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

Optionen

In diesem Fenster können Sie zusätzliche Optionen für Ihre neue Regel wählen.

Regelassistent
Optionen
Einführung
Name und Verhalten
Richtung
Dienst
Optionen
Beenden
Wählen Sie zusätzliche Optionen für diese Regel:
Regelnutzung protokollieren
Wenn die Datenpakete der Regel entsprechen, zeichnet die Firewall dies in ihrem Protokoll auf, um anzuzeigen, dass die Regel beim Filtern des Datenpakets angewandt wurde.
Die Regel außer Kraft setzen
Die Regel wird erstellt, von der Firewall aber erst nach ihrer Freigabe verwendet.
Klicken Sie unten auf den nach rechts weisenden Pfeil, um fortzufahren.
Schließen

In diesem Dialogfeld werden zwei Optionen zur Auswahl angeboten:

Regelnutzung protokollieren

Wenn Sie dieses Kontrollkästchen markieren, wird jede Anwendung der Regel protokolliert.

Die Regel außer Kraft setzen

Wenn dieses Kontrollkästchen markiert ist, wird die Regel erstellt, aber nicht aktiviert. Sie können die inaktive Regel jederzeit aktivieren.

Klicken Sie abschließend auf den nach rechts weisenden Pfeil, um das nächste Fenster zu öffnen.

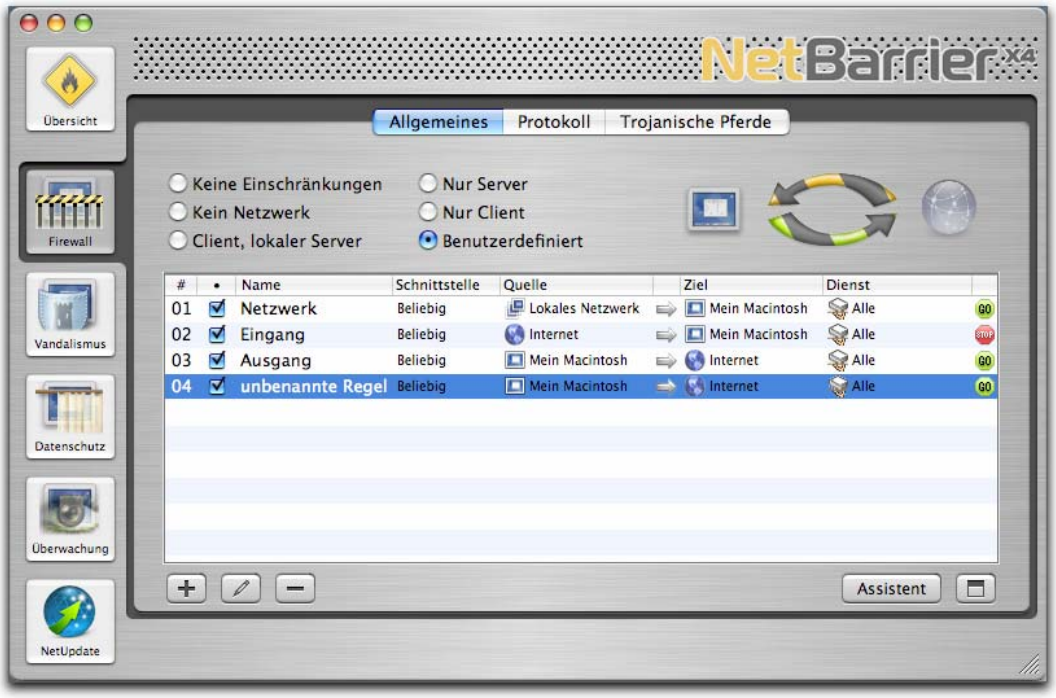
Beenden

In diesem Dialogfeld wird das Erstellen der Regel gemäß den mit dem Regelassistenten vorgenommenen Einstellungen bestätigt.

In diesem Dialogfeld wird nur eine einzige Option zur Auswahl angeboten: Wenn Sie das Kontrollkästchen „Regel für die Datenübertragung in Gegenrichtung erstellen“ markieren, erstellt der Regelassistent eine übereinstimmende Regel mit Vertauschung von Datenquelle und Datenziel.

Klicken Sie auf die Schaltfläche „Erstellen“, um eine neue Regel zu definieren und den Regelassistenten zu beenden.

Nach dem Erstellen der Regel werden Sie sehen, dass die Regel bzw. Regeln (wenn Sie das Kontrollkästchen „Regel für die Datenübertragung in Gegenrichtung erstellen“ markiert haben) in der Liste der Firewall-Regeln angezeigt wird bzw. werden.



Wenn Sie die Regel modifizieren wollen, gehen Sie bitte gemäß dem Unterabschnitt **Ändern von Regeln** weiter unten vor.

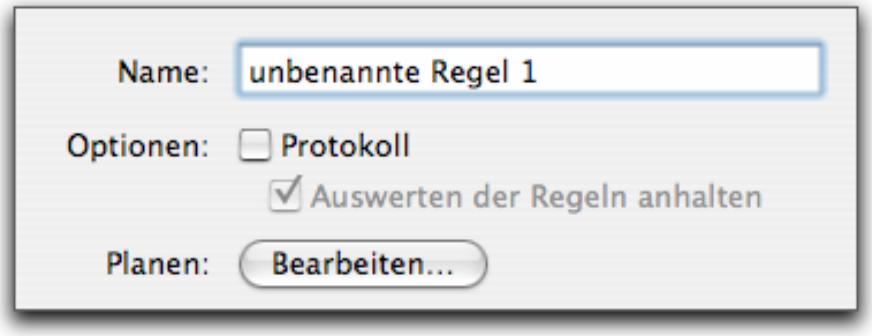
Definieren von Regeln

Im Dialogfeld „Neue Regel“ können Sie auch einzelne Regeln erstellen. Klicken Sie hierzu auf die Schaltfläche „+“. Hierauf wird das Dialogfeld „Neue Regel“ geöffnet.

In diesem Dialogfeld können Netzwerkverwalter auf einfachste Weise einen Satz von Firewall-Regeln definieren, um die Computer in dem von ihnen betreuten Netzwerk optimal vor Eindringlingen zu schützen. Die Regeln können flexibel gestaltet werden. Die Anzahl der Firewall-Regeln ist nicht begrenzt.

Im Fenster „Neue Regel“ können Firewall-Regeln auf einfachste Weise definiert werden. Sie können das Fenster ebenfalls verwenden, um vorhandene Regeln zu verändern. Das Definieren einer neuen Firewall-Regel dauert nur wenige Sekunden. Jede Regel basiert auf folgenden Elementen:

- **Der Datenquelle**
- **Dem Datenziel**
- **Dem Dienst**
- **Der Schnittstelle**
- **Der Aktion**



An der Oberseite des Fensters „Neue Regel“ befindet sich ein Textfeld, in das Sie den Namen der Regel eingeben müssen. Direkt darunter befindet sich das Kontrollkästchen für das Protokoll. Wenn dieses Kontrollkästchen markiert ist, wird der Verstoß gegen die Regel protokolliert. Wenn dieses Kontrollkästchen nicht markiert ist, werden Verstöße gegen die Regel nicht protokolliert.

Wenn das Kontrollkästchen „Protokoll“ markiert ist, so ist automatisch auch das Kontrollkästchen „Auswerten der Regeln anhalten“ markiert. Wenn dieses Kontrollkästchen markiert ist und gegen die Regel verstoßen wird, so wird die Einhaltung der darauf folgenden Regeln nicht ausgewertet. Weitere Informationen

hierzu erhalten Sie weiter unten im Abschnitt **Verwenden der Funktion „Auswerten der Regeln anhalten“**.

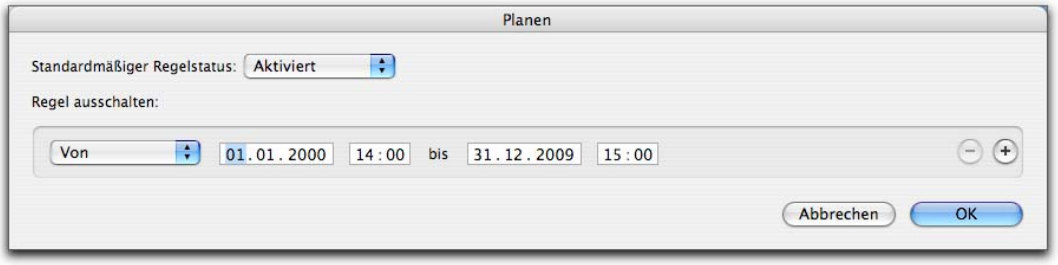
Klicken Sie auf die Schaltfläche „Bearbeiten…“, wenn Sie den Zeitplan bearbeiten möchten. Hierauf wird das Fenster „Planen“ geöffnet.

Der Regelstatus ist standardmäßig auf „Aktiviert“ eingestellt. Das heißt, Ihre Regel ist aktiviert. Wenn Sie den Status auf „Abgeschaltet“ einstellen, wendet Intego NetBarrier X4 diese Regel nicht an. Das Kontrollkästchen „Aktiviert“ ermöglicht es auch, bestimmte Regeln in eine Konfiguration aufzunehmen, aus anderen aber auszuschließen. Weitere Informationen über das Verwenden von Konfigurationssätzen finden Sie im Kapitel 6, **Voreinstellungen und Konfigurationen**.

Wenn Ihr Regelstatus standardmäßig eingeschaltet ist, können Sie bestimmte Zeitpunkte festlegen, an denen die Regel ausgeschaltet wird. Wenn Ihr Regelstatus standardmäßig ausgeschaltet ist, können Sie bestimmte Zeitpunkte festlegen, an denen die Regel eingeschaltet wird. Standardmäßig ist diese Option auf „Nie“ eingestellt. Das heißt, Ihr standardmäßiger Regelstatus wird niemals verändert. Wenn Sie die Regel für bestimmte Zeitpunkte ein- oder ausschalten möchten, klicken Sie entweder auf das Popup-Menü für „Regel aktivieren“ oder „Regel ausschalten“. Je nachdem, welchen standardmäßigen Regelstatus Sie gewählt haben. Wählen Sie dann einen der Zeitintervalle aus der Liste.

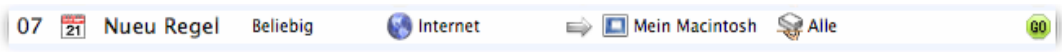
Außer der Option „Nie“ werden noch drei weitere Optionen angeboten. Mit den Optionen „Jede Woche“ und „Jeden Tag“ können Sie festlegen, ob die Regel zu einem festen, wiederkehrenden Zeitpunkt jede Woche oder jeden Tag oder nur an bestimmten Tagen der Woche ein- oder ausgeschaltet werden soll.

Sie können auch auswählen, ob die Regel für einen bestimmten Zeitraum ein- oder ausgeschaltet werden soll, indem Sie „Von“ aus dem Popup-Menü wählen. In diesem Fall müssen Sie im Feld „Von“ das Datum und die Uhrzeit festlegen, wann Ihre Regeln aktiviert werden soll. Geben Sie in das Feld „bis“ den Zeitpunkt ein, zu dem die Regel deaktiviert werden soll.



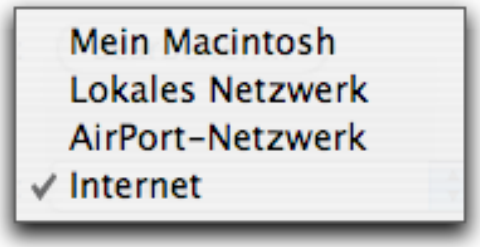
Sie können zusätzliche Zeitpunkte zum Ein- und Ausschalten der Regeln hinzufügen, indem Sie die Schaltfläche „+“ verwenden. Wenn Sie beispielsweise möchten, dass eine Regel nur montags und dienstags ausgeschaltet werden soll, können Sie diese beiden Tagen im Fenster „Planen“ festlegen. Wenn Sie einen geplanten Zeitpunkt aus der Liste entfernen möchten, klicken Sie auf die Schaltfläche „-“ neben dem Zeitpunkt, den Sie nicht länger zum Ausschalten der Regel verwenden möchten.

Geplante Regeln werden in der Regelliste mit einem Kalender-Symbol versehen.



Datenquellen

Eine Datenquelle für eine Regel ist ein Objekt, das Daten an Ihren Computer sendet. Für jede Regel kann eine von vier Datenquellen gewählt werden. Intego NetBarrier X4 ermöglicht es Ihnen nicht, in einer Regel den gleichen Computer als Datenquelle und Datenziel anzugeben.



Standardmäßig stehen vier Arten von Datenquellen zur Verfügung:

Mein Macintosh

Dies ist Ihr Computer.

Lokales Netzwerk

Dies ist ein lokales Netzwerk, mit dem Ihr Computer verbunden ist.

Airport-Netzwerk

Dies ist ein drahtloses AirPort-Netzwerk, mit dem Ihr Computer verbunden ist.

Internet

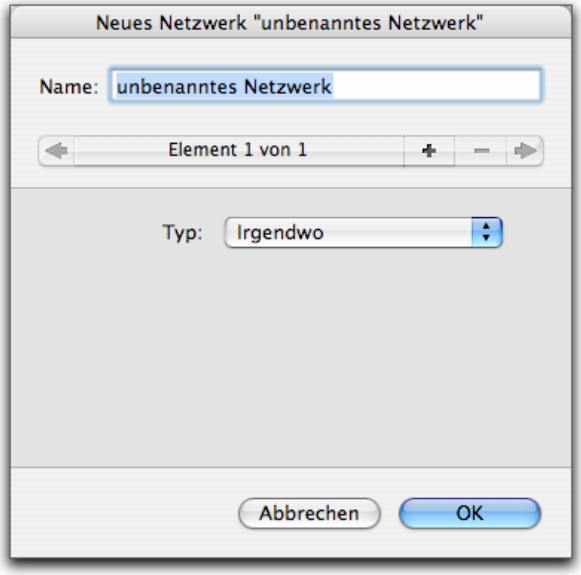
Dies ist das Internet (zusätzlich zu jedem lokalen Netzwerk, mit dem Ihr Computer verbunden sein kann). Wenn Sie die Datenquelle „Internet“ wählen, schließt dies automatisch alle anderen Netzwerke mit ein.

Definieren neuer Datenquellen

Sie können neue Datenquelle für die Verwendung in Ihren Regeln definieren. Damit können Sie exakt angeben, mit welchen Computern Ihr Computer kommunizieren darf.

Wenn Sie eine neue Datenquelle erstellen möchten, klicken Sie auf die Schaltfläche „+“ rechts neben dem Popup-Menü für Datenquellen.

Nun wird der Editor für neue Netzwerke geöffnet.



Geben Sie die folgenden Informationen ein, um eine neue Datenquelle zu definieren:

Name der Datenquelle

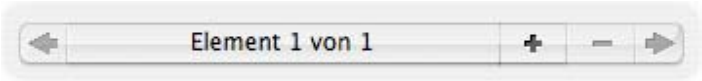
Sie können der Datenquelle einen beliebigen Namen geben, indem Sie diesen in das Textfeld „Name“ eingeben.

Datenquellenelement

Datenquellen bestehen aus mehreren Elementen. Beispielsweise können Sie mehrere IP-Nummern wählen und diese einer bestimmten Datenquelle zuordnen. Weitere Informationen hierzu finden Sie im Unterabschnitt **Adressen**.

Hinzufügen von Elementen

Um ein Element hinzuzufügen, müssen Sie aufs Symbol mit dem Schließdreieck im Abschnitt für Elemente des Fensters „Ändern des Netzwerks“ klicken.



Durchblättern der Elemente

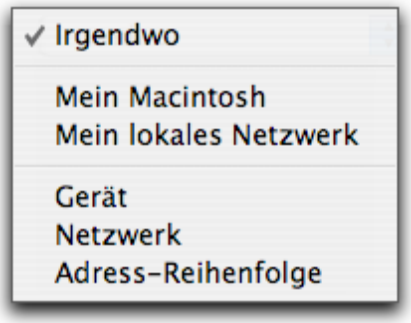
Sie können durch die Elemente blättern, indem Sie auf eine der Pfeiltasten klicken.

Löschen von Elementen

Nur ein angezeigtes Element kann gelöscht werden. Klicken Sie so oft auf eine der beiden Pfeiltasten, bis das gewünschte Element angezeigt wird. Klicken Sie auf die Schaltfläche „-“. Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Element wirklich löschen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um das Element zu löschen, und auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Netzwerktyp

Aus einem Popup-Menü können Sie sechs verschiedene Netzwerktypen wählen.



Irgendwo

Dies ist ein beliebiges Netzwerk.

Mein Macintosh

Dies ist Ihr Computer.

Mein lokales Netzwerk

Dies ist ein lokales Netzwerk, mit dem Ihr Computer verbunden ist.

Gerät

Dies ist eine spezifische IP-Nummer.

Netzwerk

Dies ist ein spezifisches Netzwerk, das durch seine IP-Nummer und seine Subnetzmaske identifiziert wird.

Adress-Reihenfolge

Dies ist eine Gruppe von IP-Nummern, die durch die Anfangs- und die Endnummer definiert ist.

Typ

Je nach dem gewählten Netzwerktyp unterscheidet sich der Adressabschnitt im Fenster „Ändern des Netzwerks“.

Irgendwo

Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie im Adressabschnitt nichts eingeben, da diese Datenquelle alle Netzwerke abdeckt.

Mein Macintosh

Wenn Sie diesen Netzwerktyp gewählt haben, wird die IP-Adresse Ihres Computers im Adressfeld angezeigt.

Mein lokales Netzwerk

Wenn Sie diesen Netzwerktyp gewählt haben, werden die Anfangs- und die Endnummer des Bereichs von IP-Nummern im Adressfeld angezeigt.

Gerät

Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie in dieses Feld die IP-Adresse eines bestimmten Computers eingeben.

Netzwerk

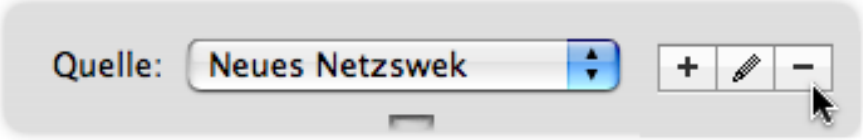
Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie die Subnetz-IP-Adresse und die Subnetzmaske des zu verwendenden Netzwerks eingeben.

Adress-Reihenfolge

Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie die Anfangs- und die Endnummer des Bereichs von IP-Nummern des zu verwendenden Netzwerks eingeben.

Löschen von Datenquellen

Sie können von Ihnen definierte Datenquellen löschen. Wählen Sie hierzu die zu löschende Datenquelle und klicken Sie dann auf die Schaltfläche „-“.

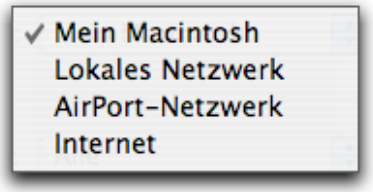


Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Netzwerk wirklich entfernen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um die Datenquelle zu löschen, und auf die Schaltfläche „Abbrechen“, um sie nicht zu löschen.

Datenziele

Ein Datenziel für eine Regel ist ein Objekt, an das Daten gesendet werden. Für jede Regel kann eines von vier Datenzielen gewählt werden. Intego NetBarrier X4 ermöglicht es Ihnen nicht, in einer Regel den gleichen Computer als Datenquelle und Datenziel anzugeben.

Standardmäßig stehen vier Arten von Datenzielen zur Verfügung:



Mein Macintosh

Dies ist Ihr Computer.

Lokales Netzwerk

Dies ist ein lokales Netzwerk, mit dem Ihr Computer verbunden ist.

Airport-Netzwerk

Dies ist ein drahtloses AirPort-Netzwerk, mit dem Ihr Computer verbunden ist.

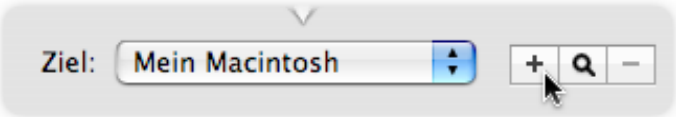
Internet

Dies ist das Internet (zusätzlich zu jedem lokalen Netzwerk, mit dem Ihr Computer verbunden sein kann). Wenn Sie die Datenquelle „Internet“ wählen, schließt dies automatisch alle anderen Netzwerke mit ein.

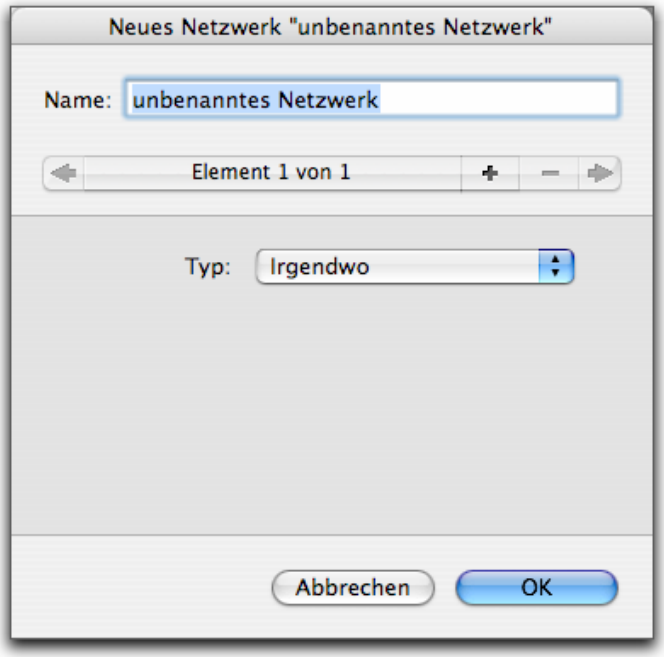
Definieren neuer Datenziele

Sie können auch neue Datenziele für Ihre Regeln definieren. Damit können Sie exakt angeben, mit welchen Computern Ihr Computer kommunizieren darf. Dienste werden auf die gleiche Weise wie Datenquellen definiert.

Wenn Sie eine neues Datenziel erstellen möchten, klicken Sie auf die Schaltfläche „+“ rechts neben dem Popup-Menü für Datenziele.



Nun wird der Editor für neue Netzwerke geöffnet.



Geben Sie die folgenden Informationen ein, um ein neues Datenziel zu definieren:

Name des Datenziels

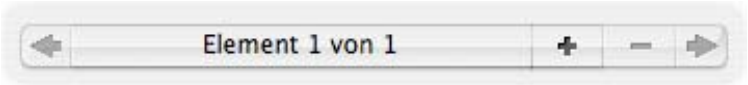
Sie können dem Datenziel einen beliebigen Namen geben, indem Sie diesen ins Textfeld eingeben.

Datenzielelement

Datenziele bestehen aus mehreren Elementen. Beispielsweise können Sie mehrere IP-Nummern wählen und diese einem bestimmten Datenziel zuordnen. Weitere Informationen hierzu finden Sie im Unterabschnitt **Adressen**.

Hinzufügen von Elementen

Um ein Element hinzuzufügen, müssen Sie auf die Schaltfläche „+“ im Abschnitt für Elemente im Editor für neue Netzwerke klicken.



Durchblättern der Elemente

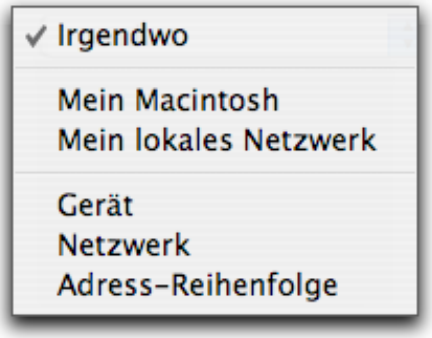
Sie können durch die Elemente blättern, indem Sie auf eine der Pfeiltasten klicken.

Löschen von Elementen

Nur ein angezeigtes Element kann gelöscht werden. Klicken Sie so oft auf eine der beiden Pfeiltasten, bis das gewünschte Element angezeigt wird. Klicken Sie auf die Schaltfläche „-“. Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Element wirklich löschen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um das Element zu löschen, und auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Netzwerktyp

Aus einem Popup-Menü können Sie sechs verschiedene Netzwerktypen wählen.



Irgendwo

Dies ist ein beliebiges Netzwerk.

Mein Macintosh

Dies ist Ihr Computer.

Mein lokales Netzwerk

Dies ist ein lokales Netzwerk, mit dem Ihr Computer verbunden ist.

Gerät

Dies ist eine spezifische IP-Nummer.

Netzwerk

Dies ist ein spezifisches Netzwerk, das durch seine IP-Nummer und seine Subnetzmaske identifiziert wird.

Adress-Reihenfolge

Dies ist eine Gruppe von IP-Nummern, die durch die Anfangs- und die Endnummer definiert ist.

Adresse

Je nach dem gewählten Netzwerktyp unterscheidet sich der Adressabschnitt im Editor für neue Netzwerke.

Irgendwo

Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie im Adressabschnitt nichts eingeben, da diese Datenquelle alle Netzwerke abdeckt.

Mein Macintosh

Wenn Sie diesen Netzwerktyp gewählt haben, wird die IP-Adresse Ihres Computers im Adressfeld angezeigt.

Mein lokales Netzwerk

Wenn Sie diesen Netzwerktyp gewählt haben, werden die Anfangs- und die Endnummer des Bereichs von IP-Nummern im Adressfeld angezeigt.

Gerät

Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie in dieses Feld die IP-Adresse eines bestimmten Computers eingeben.

Netzwerk

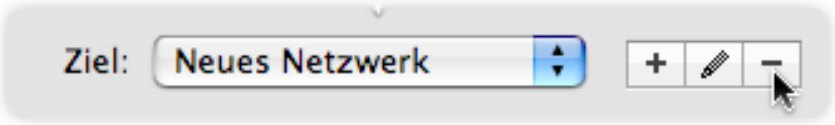
Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie die Subnetz-IP-Adresse und die Subnetzmaske des zu verwendenden Netzwerks eingeben.

Adress-Reihenfolge

Wenn Sie diesen Netzwerktyp gewählt haben, müssen Sie die Anfangs- und die Endnummer des Bereichs von IP-Nummern des zu verwendenden Netzwerks eingeben.

Löschen von Datenzielen

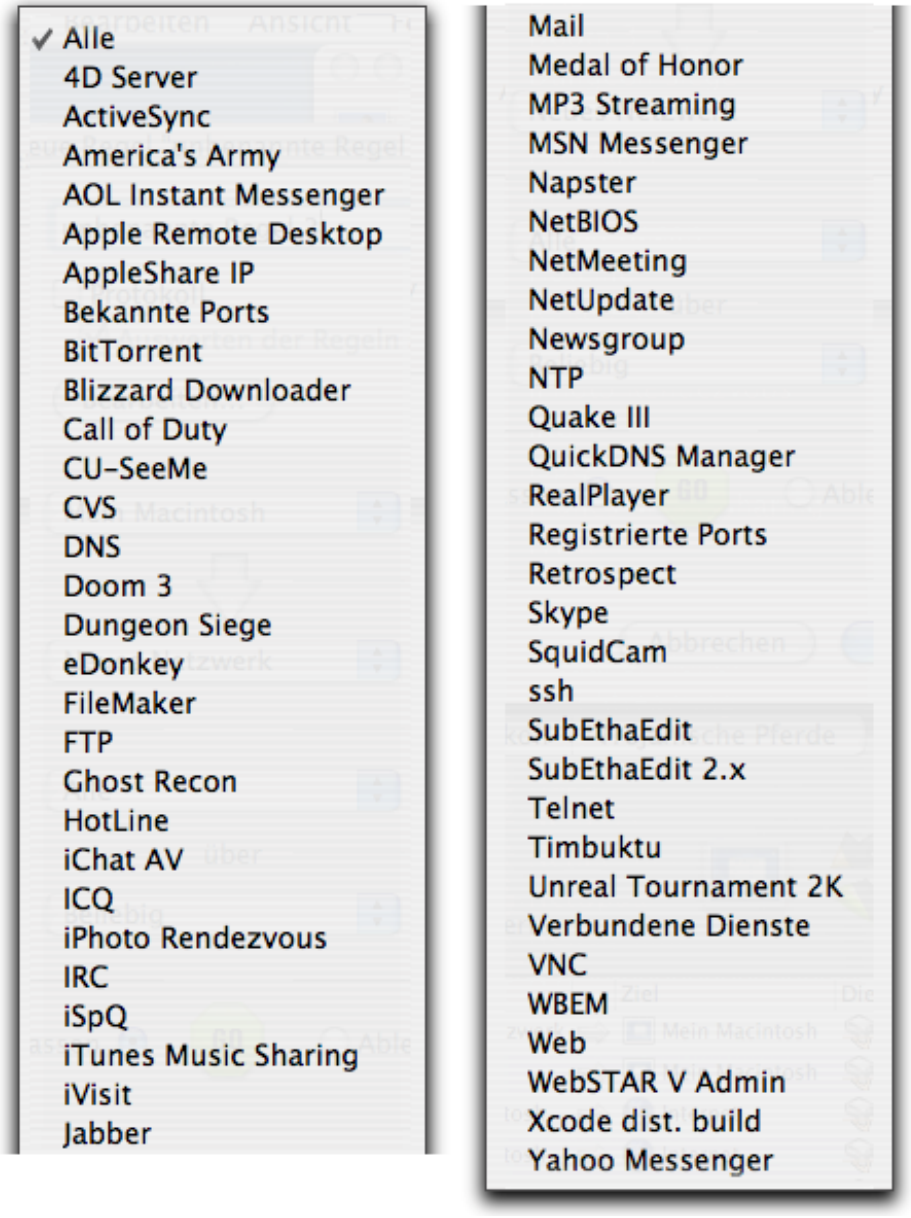
Sie können von Ihnen definierte Datenziele löschen. Wählen Sie hierzu das zu löschende Datenziel und klicken Sie dann auf die Schaltfläche „-“.



Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Datenziel wirklich entfernen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um das Datenziel zu löschen, und auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Dienste

Standardmäßig stehen mehrere Dienste zur Verfügung:



Alle

Wenn Sie diese Option gewählt haben, wird die Regel für alle Arten von Diensten aktiviert.

E-Mail

Wenn Sie diese Option gewählt haben, wird die Regel nur für den Dienst „E-Mail“ aktiviert.

FTP

Wenn Sie diese Option gewählt haben, wird die Regel nur für den Dienst „FTP“ aktiviert.

Web

Wenn Sie diese Option gewählt haben, wird die Regel nur für den Dienst „HTTP“ (Zugriff aufs World Wide Web) aktiviert.

Verbundene Dienste

Wenn Sie diese Option gewählt haben, wird die Regel nur für TCP-Dienste aktiviert.

Bekannte Ports

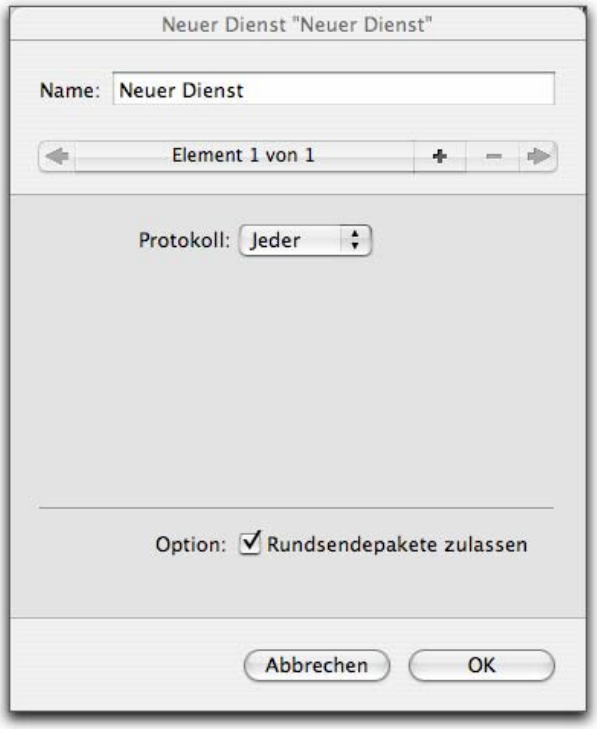
Wenn Sie diese Option gewählt haben, wird die Regel für bekannte Ports aktiviert. Diese Ports werden von häufig verwendeten Anwendungsprogrammen genutzt.

Die restlichen Dienste sind nur für bestimmte Anwendungsprogramme oder Protokolle relevant.

Definieren neuer Dienste

Sie können auch neue Dienste für Ihre Regeln definieren. Damit können Sie exakt angeben, welche Dienste Ihr Computer akzeptieren und/oder verwenden darf. Dienste werden auf die gleiche Weise wie Datenquellen definiert.

Wenn Sie einen neuen Dienst erstellen möchten, klicken Sie auf die Schaltfläche „+“ rechts neben dem Popup-Menü für Dienste. Nun wird der Editor für neue Dienste geöffnet.



Geben Sie die folgenden Informationen ein, um einen neuen Dienst zu definieren:

Name des Dienstes

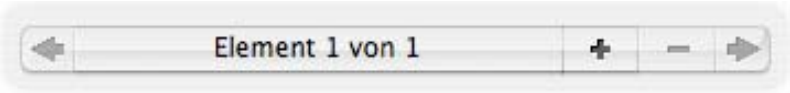
Sie können dem Dienst einen beliebigen Namen geben, indem Sie diesen in das Textfeld „Name“ eingeben.

Diensteelement

Dienste bestehen aus mehreren Elementen. Beispielsweise können Sie mehrere Dienste wählen und diese einer bestimmten Regel zuordnen.

Hinzufügen von Elementen

Um ein Element hinzuzufügen, müssen Sie aufs Symbol mit dem Schließdreieck im Abschnitt für Elemente des Fensters „Ändern von Diensten“ klicken.



Durchblättern der Elemente

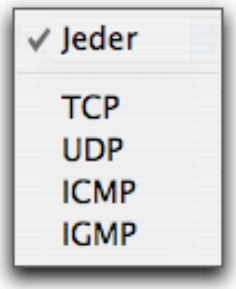
Sie können durch die Elemente blättern, indem Sie auf eine der Pfeiltasten klicken.

Löschen von Elementen

Nur ein angezeigtes Element kann gelöscht werden. Klicken Sie so oft auf eine der beiden Pfeiltasten, bis das gewünschte Element angezeigt wird. Klicken Sie auf die Schaltfläche „-“. Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Element wirklich löschen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um das Element zu löschen, und auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Protokoll

Aus dem Popup-Menü können Sie vier unterschiedliche Protokollgruppen wählen: TCP, UDP, ICMP und IGMP. Sie können auch die Option „Jeder“ wählen, in die sämtliche Kommunikationsprotokolle eingeschlossen sind.



Wenn Sie eine dieser Protokollgruppen wählen, werden im unteren Teil des Fensters weitere Optionen mit einer Liste der wählbaren Dienste angezeigt. Diese Optionen ändern sich je nach dem gewählten Kommunikationsprotokoll. Weitere Informationen über die Kommunikationsprotokolle und Dienste finden Sie im Kapitel 9, **Häufig verwendete Fachbegriffe**.

Port oder **Typ**

Bei der Auswahl des Ports für TCP- bzw. UDP-Dienste oder des Typs für ICMP- oder IGMP-Dienste bestehen zwei Möglichkeiten.

Jeder Port oder **Jeder Typ**

Wenn Sie diese Option gewählt haben, wird die Regel für alle Arten von Ports oder Typen aktiviert.

Spezifischer Port oder **Spezifischer Typ**

Sie können auch die Port-Nummer oder den Typ angeben. Bei der Auswahl anderer Dienste werden in dieses Feld automatisch deren standardmäßige Port-

Nummern eingetragen. Wenn Sie eine andere Port-Nummer verwenden müssen, können Sie diese manuell eingeben.

Reihe von Ports

Bei TCP- und UDP-Diensten können Sie auch einen Portbereich angeben. Wenn Sie eine Reihe von Ports wählen, müssen Sie in die Felder „Von Port“ und „Bis Port“ die niedrigsten und die höchsten Port-Nummern eingeben, die Sie verwenden wollen.

Rundsendepakete zulassen

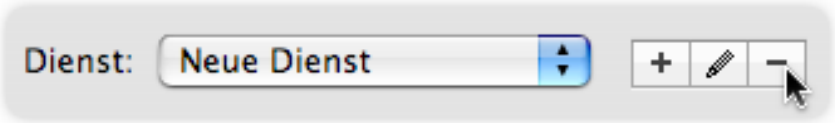
Wenn dieses Kontrollkästchen markiert ist, werden Rundsendepakete (d.h. Datenpakete, die an alle Computer in einem Netzwerk gesendet werden), in diesen Dienst aufgenommen.

Ziel-Port

Diese Option steht für das UDP-Protokoll zur Verfügung. Wenn diese Option markiert ist, werden Pakete je nach Funktion des Ziel-Ports gefiltert. Wenn diese Option nicht markiert ist, werden Pakete je nach Funktion des Quell-Ports gefiltert.

Löschen von Diensten

Sie können von Ihnen definierte Dienste löschen. Wählen Sie hierzu den zu löschenden Dienst und klicken Sie dann aufs Papierkorbsymbol.



Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie diesen Dienst wirklich entfernen wollen. Falls Sie dies wollen, müssen Sie auf die Schaltfläche „Ja“ klicken. Klicken Sie andernfalls auf die Schaltfläche „Abbrechen“.

Schnittstellen

Eine Schnittstelle für eine Regel ist die Netzwerkkarte, über die Ihr Computer mit anderen Computern kommuniziert. Hierbei kann es sich um eine Ethernet-Karte, eine AirPort-Karte (für drahtlose Kommunikation Ihres Computers), eine PPP-Verbindung oder eine andere Art von Netzwerkschnittstelle handeln. Sie können eine der vorhandenen Netzwerkschnittstellen Ihres Computers wählen oder Ihre eigene Netzwerkschnittstelle definieren.

Schnittstellentyp

Aus einem Popup-Menü können Sie sechs verschiedene Netzwerkschnittstellen wählen. Dieses Menü bietet Ihnen unter anderem folgende Optionen zur Auswahl an:

Jeder

Dies ist jeder Schnittstellentyp an Ihrem Computer.

Integriertes Ethernet

Dies ist die eingebaute Ethernet-Karte (sofern vorhanden).

AirPort

Dies ist die AirPort-Karte (sofern vorhanden).

Definieren neuer Schnittstellen

Sie können neue Schnittstellen für die Verwendung in Ihren Regeln definieren. Wenn Sie eine neue Schnittstelle erstellen möchten, klicken Sie auf die Schaltfläche „+“ rechts neben dem Popup-Menü für Schnittstellen.

Nun wird der Editor für neue Schnittstellen geöffnet.

Geben Sie die folgenden Informationen ein, um eine neue Schnittstelle zu definieren:

Name der Schnittstelle

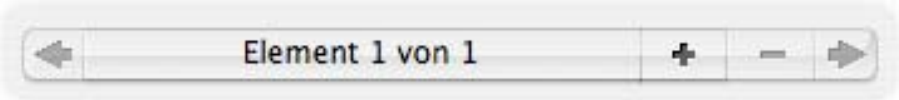
Sie können der Schnittstelle einen beliebigen Namen geben, indem Sie diesen in das Textfeld „Name“ eingeben.

Schnittstellenelement

Schnittstellen bestehen unter Umständen aus mehreren Elementen. Sie können beispielsweise mehrere Schnittstellen in eine Schnittstelle der höheren Ebene integrieren, womit Sie sicherstellen können, dass sich eine Regel gleichzeitig auf mehrere Schnittstellen auswirkt.

Hinzufügen von Elementen

Um ein Element hinzuzufügen, müssen Sie aufs Symbol mit dem Schließdreieck im Abschnitt für Elemente des Fensters „Ändern des Netzwerks“ klicken.



Durchblättern der Elemente

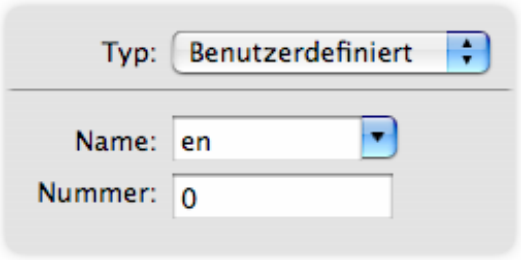
Sie können durch die Elemente blättern, indem Sie auf eine der Pfeiltasten klicken.

Löschen von Elementen

Nur ein angezeigtes Element kann gelöscht werden. Klicken Sie so oft auf eine der beiden Pfeiltasten, bis das gewünschte Element angezeigt wird. Klicken Sie auf die Schaltfläche „-“. Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie dieses Element wirklich löschen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um das Element zu löschen, und auf die Schaltfläche „Abbrechen“, um es nicht zu löschen.

Schnittstellentyp

Aus einem Popup-Menü können Sie die Option „Jede“ oder „Benutzerdefiniert“ wählen. Wenn Sie eine spezielle Schnittstelle definieren wollen, müssen Sie auf die Schaltfläche „Benutzerdefiniert“ klicken.



Wählen Sie den Namen Ihrer Schnittstelle und geben Sie deren Nummer ein. Klicken Sie dann auf die Schaltfläche „OK“, um die Einstellungen zu speichern.

Löschen von Schnittstellen

Sie können von Ihnen definierte Schnittstellen löschen. Wählen Sie hierzu die zu löschende Schnittstelle und klicken Sie dann auf die Schaltfläche „-“.

Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie diese Schnittstelle wirklich entfernen wollen. Klicken Sie auf die Schaltfläche „Entfernen“, um die Schnittstelle zu löschen, und auf die Schaltfläche „Abbrechen“, um sie nicht zu löschen.

Aktionen

Bei Verstoß gegen eine Regel sind zwei Aktionen möglich: „Zulassen“ oder „Verweigern“. Wählen Sie die gewünschte Aktion für Ihre Regel, indem Sie aufs entsprechende runde Optionsfeld an der Unterseite des Fensters „Ändern von Regeln“ klicken. Klicken Sie auf „OK“, wenn Sie diese Regel den Firewall-Regeln von NetBarrier X4 hinzufügen möchten.

Dienste-Bibliothek

Regeln können auch mit der Dienste-Bibliothek erstellt werden. Sie können sich die Dienste-Bibliothek anzeigen lassen, indem Sie auf das entsprechende Symbol in der unteren rechten Ecke des Abschnitts „Firewall“ klicken.

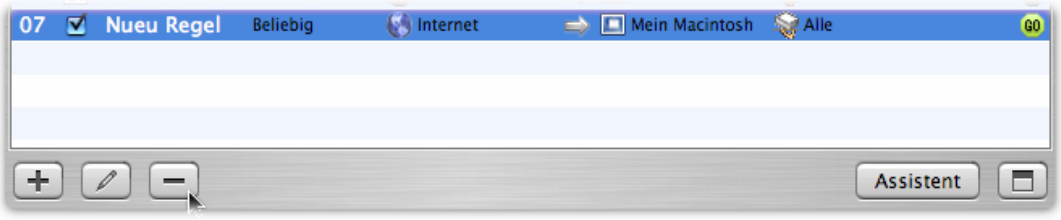
Hierauf wird das Fenster „Dienste-Bibliothek“ geöffnet, in dem Ihnen eine Liste verschiedener Dienste angezeigt wird, die für Ihren Computer verwendet werden können. Sie können das Dropdown-Menü verwenden, um sich die vollständige Diensteliste oder einen bestimmten Satz von Diensten anzeigen zu lassen.

Wenn Sie eine neue Regel erstellen möchten, wählen Sie den gewünschten Dienst aus und ziehen Sie ihn in die Regelliste. Sie können die Einstellungen für die Regel

bearbeiten, indem Sie die Regel auswählen und dann auf die Schaltfläche mit dem Bleistiftsymbol unterhalb der Regelliste klicken. Die verschiedenen Einstellungsmöglichkeiten wurden bereits zuvor in diesem Abschnitt erklärt.

Löschen von Regeln

Wenn Sie eine Regel löschen möchten, wählen Sie die Regel aus der Regelliste, indem Sie darauf klicken und klicken Sie anschließend auf die Schaltfläche „-“. Hierauf wird ein Dialogfeld geöffnet, in dem Sie gefragt werden, ob Sie diese Regel wirklich löschen wollen. Klicken Sie auf die Schaltfläche „OK“. Wenn Sie diese Regel nicht löschen wollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.

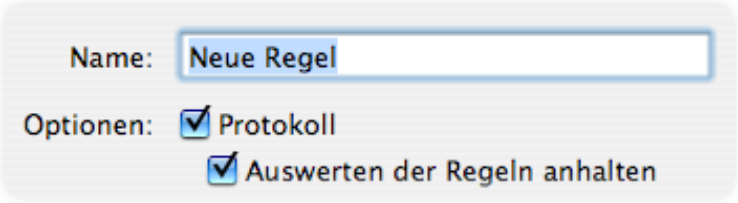


Ändern von Regeln

Wenn Sie eine Regel bearbeiten wollen, müssen Sie auf den Namen der Regel und dann auf die Schaltfläche mit dem Bleistiftsymbol klicken. Hierauf wird der Regel-Editor geöffnet, in dem Sie alle gewünschten Änderungen an dieser Regel vornehmen können. Klicken Sie nach Abschluss der Änderungen auf die Schaltfläche „OK“, um die Änderungen wirksam werden zu lassen. Wenn die Änderungen nicht wirksam werden sollen, müssen Sie auf die Schaltfläche „Abbrechen“ klicken.

Verwenden der Funktion „Auswerten der Regeln anhalten“

Wenn Sie eine Regel erstellen und das Kontrollkästchen „Protokoll“ markiert ist, wird auch das Kontrollkästchen „Auswerten der Regeln anhalten“ markiert. Dieses Kontrollkästchen wird automatisch markiert. Wenn Sie das Kontrollkästchen markiert lassen, wird nicht auf Einhaltung der darauf folgenden Regeln geprüft.



Wenn Sie dieses Kontrollkästchen nicht markieren, können Sie eine Regel definieren, sodass bei einem Verstoß gegen sie ein- oder ausgehender Datenverkehr protokolliert wird, ohne dass der Datenverkehr behindert wird. Wenn die IP-Adresse oder der Dienst mit dem gleichen Element in der Regel übereinstimmt und das Kontrollkästchen „Auswerten der Regeln anhalten“ nicht markiert ist, wird der Datenverkehr protokolliert, aber nicht gesperrt.

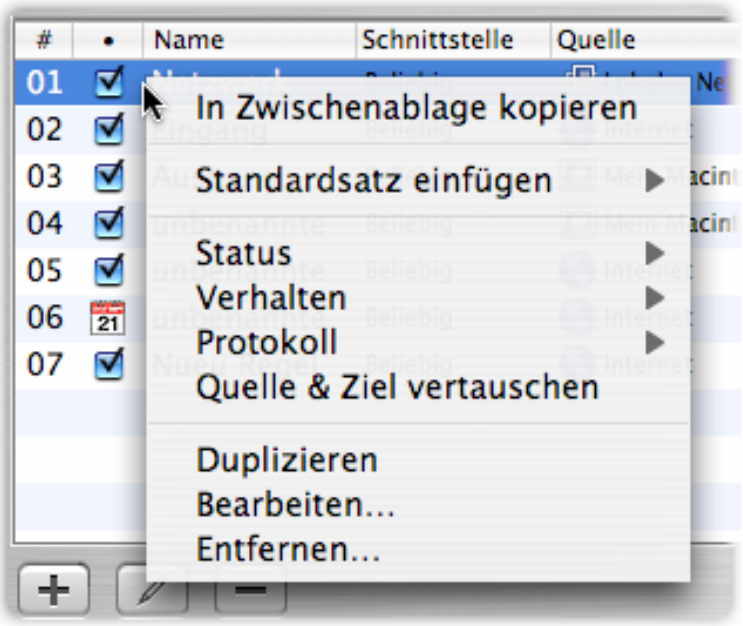
Anmerkung: Gehen Sie beim Definieren von Regeln für bestimmte Dienste vorsichtig vor. Wenn Sie einen Dienst für ein bestimmtes Programm wählen, kann es vorkommen, dass dieses Programm den gleichen Port wie ein anderes Programm oder ein anderer Dienst verwendet. Durch das Sperren oder Freigeben eines Dienstes kann ein Konflikt mit anderen, allgemeineren Regeln entstehen. Wenn Sie beispielsweise ICQ-Datenverkehr sperren wollen, wird durch die Auswahl des Dienstes ICQ auch der Datenverkehr mit Hilfe des Programms „AOL Instant Messenger“ gesperrt, da diese beiden Programme den gleichen Port verwenden. Andere Programme verwenden unter Umständen ebenfalls die gleichen Ports. Wenn Sie erkennen, dass Sie keine Verbindung mit einem bestimmten Dienst herstellen oder keine Datenpakete senden oder empfangen

können, sollten Sie die von Ihnen selbst definierten Regeln nacheinander außer Kraft setzen, um zu sehen, ob hier ein Konflikt besteht.

Verwenden des Kontextmenüs für Regeln

Ein Kontextmenü vereinfacht das Arbeiten mit Firewall-Regeln. Über dieses Menü haben Sie Zugriff auf viele Regelfunktionen. Mit Hilfe des Kontextmenüs können Sie Regeln mit einem einzigen Mausklick ändern. Sie können dieses Kontextmenü dazu verwenden, um neue Regeln hinzuzufügen, bereits definierte Regeln zu ändern und die Eigenschaften von Regeln zu ändern.

Dieses Kontextmenü wird bei gedrückter Taste „ctrl“ in der Tastatur Ihres Macintosh geöffnet. Sie müssen nun nur noch auf den Namen einer Regel klicken. (Wenn Sie eine Maus mit zwei Tasten verwenden, können Sie auch auf die rechte Maustaste klicken, um das Kontextmenü zu öffnen.)



Das Kontextmenü bietet folgende Optionen zur Auswahl an:

In Zwischenablage kopieren

Damit können Sie den Inhalt einer Regel in die Zwischenablage kopieren.

Standardsatz einfügen/Standardsatz hinzufügen

Hiermit können Sie einen Standardsatz von Regeln ein- oder hinzufügen. Im Untermenü „Standardsatz einfügen“ haben Sie die Auswahl aus fünf Regelsätzen: „Keine Einschränkungen“, „Kein Netzwerk“, „Client, lokaler Server“, „Nur Server“ und „Nur Client“.

Status

Sie können eine Regel aktivieren oder abschalten. Wenn die Regel so geplant wurde, dass sie zu bestimmten Zeitpunkten ausgeführt wird, wird neben „Geplant“ eine Markierung angezeigt.

Verhalten

Sie können das Verhalten einer Regel von „Zulassen“ auf „Verweigern“ (von Datenverkehr) und umgekehrt umschalten.

Protokoll

Sie können definieren, ob eine Regel Datenverkehrsinformationen im Protokoll aufzeichnen lassen soll.

Quelle & Ziel vertauschen

Hierdurch werden die Datenquelle und das Datenziel einer Regel vertauscht.

Duplizieren

Hiermit wird eine Kopie der Regel angelegt.

Bearbeiten…

Diese Option ermöglicht das Ändern einer Regel im Dialogfeld „Ändern von Regeln“.

Entfernen…

Hiermit können Sie eine Regel löschen.

8 – Technische Unterstützung

Als registrierter Intego-Kunde erhalten Sie von Intego technische Kundenunterstützung.

Per E-Mail

eurosupport@intego.com: Europa, Naher Osten, Afrika

support@intego.com: Nord- und Südamerika

supportfr@intego.com: Frankreich

supportjp@intego.com: Japan

Über die Intego-Website

www.intego.com

Anerkennungen

Teile dieser Intego-Software können eventuell die folgenden Materialien verwenden, die durch Copyright geschützt sind. Die Verwendung derselben wird hierdurch anerkannt.

EDCommon und EDInternet Frameworks, geschrieben von Erik Dörnenburg.

Omni Development (OAGradientTableView)
Copyright 2003-2004 Omni Development, Inc. Alle Rechte vorbehalten.

9 – Glossar

Adressmaske: Eine Bitmaske zur Identifizierung, welche Bits in einer IP-Nummer mit der Netzwerkadresse und Subnetzelementen der Adresse übereinstimmen.

Adressmaskenantwort: Eine Antwort auf eine Adressmaskenabfrage.

Adressmaskenabfrage: Ein Befehl zum Abfragen einer Adressmaske.

Bootp: Das Urladeprotokoll. Dieses Protokoll wird zum Starten von Arbeitsplatzcomputern verwendet, die über keine eigene Massenspeichereinheit verfügen.

Bootp-Client: Ein Computer, der als Bootp-Client arbeitet.

Bootp-Server: Ein Computer, der als Bootp-Server arbeitet.

Rundsendepaket: In einem Ethernet-Netzwerk ist ein Rundsendepaket ein spezielles Datenpaket für den Empfang durch mehrere Datenziele, das von alle Knotenpunkten des Netzwerks empfangen wird.

Chat: Ein Dialogsystem, das es mehreren angemeldeten Teilnehmern ermöglicht, über ein Netzwerk zu kommunizieren, indem sie Informationen in ein Fenster tippen, die dann von den anderen Teilnehmern gesehen werden können. Die Aktualisierung dieser Informationen erfolgt häufig oder in Echtzeit.

Client: Ein Computersystem oder Prozess, das bzw. der einen Dienst von einem anderen Computersystem oder Prozess (einem Server) anfordert. Ein Arbeitsplatzcomputer, der eine Datei von einem Dateiserver anfordert, ist der Client dieses Servers.

Senden einer großen Anzahl von Verbindungsanforderungen: Ein Angriff auf einen Computer, bei dem der sendende Computer den empfangenden Computer förmlich mit einer Flut von Datenpaketen überschwemmt, um Verbindungen mit ihm herzustellen. Dadurch wird der empfangende Computer überlastet und ist nicht mehr in der Lage, seine eigentlichen Tätigkeiten auszuüben.

Cookie: Hierbei handelt es sich um eine kleine Datei, die ein Website-Server auf der Festplatte Ihres Computers speichert. Beim nächsten Besuch der gleichen Website wird das Cookie von Ihrem Webbrowser an eben diesen Website-Server zurückgesandt. Typischerweise werden Cookies dazu verwendet, um einen Benutzer wieder zu

erkennen, nachdem er sich einmal bei einer Website angemeldet hat. Dadurch müssen die Anmeldeinformationen wie Benutzername und Passwort nicht mehr eingegeben werden. Cookies werden auch dazu verwendet, um den Einkauf im Internet zu vereinfachen. So können Sie zunächst Ware auf einer Website auswählen und in einen virtuellen „Einkaufswagen“ legen. Dank dem Cookie weiß der Website-Server später, welche Produkte oder Dienstleistungen Sie erwerben wollen, bevor es an die Bezahlung geht. Ein Cookie ermöglicht es auch, zu erkennen, welche Seiten einer Website Sie aufgerufen haben, sodass Ihnen auf Ihre persönlichen Vorlieben abgestimmte Seiten angeboten werden.

Datentelegramm: Ein autonomes Datenpaket, das ausreichend viele Informationen enthält, um unabhängig von früheren und späteren Datentransfers von der Datenquelle zum Datenziel transportiert zu werden.

Datentelegrammumsetzungsfehler: Ein Fehler bei der Datentelegrammumsetzung.

DNS: Domain Name System = Domänennamensystem. Ein von Routern im Internet verwendetes System zur Übersetzung von Domänennamen wie z.B. www.intego.com in die IP-Nummern (die eigentlichen Internet-Adressen) von Servern.

Echo: Eine während einer Ping-Aktion gesendete Abfrage.

Echoantwort: Die Antwort auf eine Echoabfrage.

Finger: Ein Programm zur Abfrage von Informationen über einen Benutzer im Internet oder einem anderen Netzwerk.

FTP: File Transfer Protocol = Dateitransferprotokoll. Ein Protokoll für die Übertragung von Dateien von einem Computer auf einen anderen. Für den Dateitransfer wird entweder ein Webbrowser oder ein spezielles FTP-Programm verwendet.

Gopher: Ein verteiltes Dokumentenabfragesystem (ein Vorläufer des World Wide Web).

Host: Eigentliche Bedeutung dieses englischen Begriffs: Gastgeber oder Wirt. In der Informationstechnologie ein mit einem Netzwerk verbundener Computer.

HTTP: HyperText Transfer Protocol = HyperText-Transferprotokoll. Dieses Protokoll ermöglicht die Übertragung von Website-Inhalten im World Wide Web.

ICMP: Internet Control Message Protocol = Internet-Protokoll für Status- und Kontrollmeldungen. Dieses Protokoll regelt die Aktionen von Fehler- und Kontrollmeldungen die während einer Datenübertragung von den beteiligten Computern ausgetauscht werden.

IGMP: Internet Group Management Protocol = Internet-Protokoll für die Gruppenunterstützung.

IMAP4: Internet Message Access Protocol = Internet-Protokoll für den Zugriff auf Nachrichten. Dieses Protokoll ermöglicht einem Computer den Zugriff und die Verwaltung von E-Mail-Mitteilungen auf einem Mailserver. Die E-Mail-Mitteilungen können in Ordnern auf dem Mailserver verwaltet werden, wie dies mit E-Mail-Programmen auf einem Arbeitsplatzcomputer möglich ist.

Intranet-Datenwegelenkung: Die Auswahl der korrekten Schnittstelle und der nächsten Zwischenstation bei der Weiterleitung eines Datenpakets durch ein Intranet. Die Datenwegelenkung wird von einem Router übernommen.

IP: Internet Protocol = Internet-Protokoll. Die Netzwerkschicht des weit verbreiteten TCP/IP-Protokolls für die Datenübertragung in Ethernet-Netzwerken und im Internet.

Internet-Adresse: Die Adresse eines Computers, der das Internet-Protokoll (IP) verwendet.

IRC: Internet Relay Chat = Internet-Relaisdialog. Ein Medium für die weltweite Echtzeitkommunikation vieler Teilnehmer übers Internet.

LAN: Local Area Network = lokales Netzwerk. Ein Netzwerk, über das mehrere Computer in einem örtlich begrenzten Bereich miteinander verbunden sind. Unter einem „örtlich begrenzten Bereich“ ist beispielsweise ein Gebäude, eine Werksgelände, ein Universitätsgelände oder ähnlich zu verstehen.

NETBIOS: Network Basic Input/Output System = Basis-Eingabe- und -Ausgabesystem für Netzwerke. Eine Softwareschicht, die ursprünglich für die Verbindung eines Netzwerkbetriebssystems mit spezifischer Hardware vorgesehen war. NETBIOS kann auch die Kommunikation zwischen Arbeitsplatzcomputern in einem Netzwerk in der Transportschicht eröffnen.

Netzwerk: Eine Verbindung mehrerer Computer, die so miteinander verbunden sind, dass sie Daten untereinander austauschen können. Bei einem Netzwerk kann es sich um ein LAN oder um ein großes Netzwerk wie z.B. das Internet handeln.

NNTP: Network News Transfer Protocol = Netzwerknachrichten-Transferprotokoll. Ein Protokoll zum Verteilen, Abfragen, Abholen und Versenden von Diskussionsbeiträgen in Newsgroup übers Internet.

NTP: Network Time Protocol = Netzwerk-Zeitprotokoll. Dieses Protokoll stellt übers Internet die Synchronisation der in Computern eingebauten Echtzeituhren mit Funk-, Atom- oder anderen Uhren sicher. Dieses Protokoll ist in der Lage, geografisch verteilte Uhren langfristig mit einer Abweichung von nur wenigen Millisekunden zu synchronisieren.

Datenpaket: Eine Dateneinheit, die über Netzwerke von einem Computer zu einem anderen übertragen wird. Ein Datenpaket enthält die Adresse des Absenders und des Empfängers, die Nutzdaten und andere Informationen.

Ping: Ein Programm zum Prüfen der Erreichbarkeit von Computern über ein Netzwerk. Das Programm sendet eine Echoabfrage und wartet auf eine Antwort.

Ping-Rundsenden: Ein Angriff ähnlich wie eine Ping-Überflutung. Siehe unten.

Ping-Überflutung: Ein Ping-Angriff auf einen Computer, wobei der Sender den Empfänger mit einer Flut von Echoabfragen überschwemmt. Dadurch wird der empfangende Computer überlastet und ist nicht mehr in der Lage, seine eigentlichen Tätigkeiten auszuüben.

Ping Of Death: Ein besonders gefährlicher Ping-Angriff, der zum Absturz des empfangenden Computers führen kann.

POP3: Post Office Protocol (Postamtprotokoll), Version 3. POP3 ermöglicht es einem Client-Computer, E-Mail-Mitteilung von einem POP3-Server abzuholen.

Port-Scan: Das Abfragen der Ports eines Computers durch einen Eindringling, um herauszufinden, welche Dienste am angegriffenen Computer zur Verfügung stehen.

Protokoll: Ein Regelwerk für den Datenaustausch zwischen Computern in einem Netzwerk. Für den Datenaustausch im Internet stehen mehrere Protokolle (IP, HTTP, FTP, NNTP usw.) zur Verfügung.

Router: Eine Hardwareeinheit oder eine Software für die Weiterleitung von Datenpaketen zwischen Netzwerken, wobei der Router die Adressinformationen aus den Datenpaketen ausliest.

Server: Ein Server (= Diener) ist ein Computer, der mit einem Netzwerk verbunden ist, und dessen Aufgabe darin besteht, anderen Computern im Netzwerk Daten oder Dateien zur Verfügung zu stellen. Diese anderen Computer werden als „Clients“ (= Kunden) bezeichnet.

Dienst: Eine auf einem Server zur Verfügung stehende Netzwerkfunktion wie z.B. HTTP, FTP, E-Mail usw.

SMTP: Simple Mail Transfer Protocol = einfaches Postübertragungsprotokoll. Ein Protokoll zum Übertragen von E-Mail-Mitteilungen zwischen Computern.

Spam: Unaufgefordert empfangene E-Mail-Mitteilungen (hauptsächlich per E-Mail zugesandte Werbemitteilungen, die gleichzeitig an Tausende oder sogar Millionen von Internet-Benutzern versandt werden, um Produkte oder Dienstleistungen zu verkaufen.

TCP: Transmission Control Protocol = Sendesteuerungsprotokoll. Das meistverwendete Datentransferprotokoll in Ethernet-Netzwerken und im Internet.

TCP/IP: Die Internet-Version von TCP: TCP über IP.

Telnet: Das standardmäßige Internet-Protokoll fürs Anmelden bei entfernten Computern.

TFTP: Trivial File Transfer Protocol = triviales Dateitransferprotokoll. Ein einfaches Dateitransferprotokoll fürs Herunterladen des Urladeprogrammcodes auf Arbeitsplatzcomputer ohne eigene Massenspeichereinheit.

Traceroute: Ein Dienstprogramm zum Verfolgen von Datenpaketen auf ihrem Weg von einem Computer zu einem anderen.

UDP: User Datagram Protocol = Benutzer-Datentelegramm-Protokoll. Ein Internet-Protokoll, das einfache, aber fehleranfällige Datentelegrammdienste zur Verfügung stellt.

Whois: Ein Internet-Verzeichnisdienst zum Suchen von Informationen über Domänennamen und IP-Nummern.